Council of the European Union
General Secretariat

Interinstitutional files:
2025/0360 (COD)

Brussels, 19 March 2026

WK 3736/2026 ADD 1

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV
COMPET
MI

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Antici Group (Simplification)
Subject:	Consultation on Omnibus VII (GDPR/P2B/ePrivacy) Digital rules - related to AGS meeting of 27.02.26 (deadline 18.03.26) - consolidated written comments on GDPR/P2B & ePrivacy files - 13 Member States

Delegations will find attached two files with consolidated comments from our templates, submitted by the following Member States: **AT, ES, LV and SE** (for GDPR/P2B) and the Member States who have submitted comments for the consolidated file (ePrivacy) as follows: **BE, CZ, DK, FI, IE, IT, LU, NL and SI.**

Digital omnibus on GDPR/P2B Deadline: ***18 March 2026***
From: AT, ES, LV, SE **Updated: 19/03/2026 16:11**

Guidelines to be followed

Please kindly provide your contributions in the table below.

Drafting suggestions: you may use '**track changes**'* or formatting (for example **bold-underline** for additions and ~~strike-through~~ for deletions, **where necessary, in a different colour**). *Track changes can only be connected once the cursor is placed in editable areas (Drafting or Comments columns).

To make it feasible to consolidate all contributions, the structure of the table must not be changed, so **no rows can be added or deleted.**

New provisions may only be added in any of the **'existing cells'.**

Name of document: please add the **two initials** of your delegation's country followed by a space (to the MS Word document name), followed by any optional text, for example, for Austria: **AT comments on … .docx**

Thank you for your cooperation!

Presidency compromise text	Drafting suggestions and Comments
General Comments	LV (Comments): LV expresses concern regarding the proposed expansion of the derogations allowing the processing of special categories of personal data for the purposes of developing and operating an AI system. LV notes, in particular, that introducing a sector- specific derogation limited to a single technological domain risks undermining the principle of technological neutrality embedded in the GDPR and may lead to legal fragmentation. LV also considers that the proposed Articles 88a, 88b and 88c raise concerns regarding the systemic coherence and the principle of technological neutrality of the GDPR. LV specific concerns and drafting suggestions are set out below in relation to the individual provisions.

Presidency compromise text	Drafting suggestions and Comments
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2022/2554, and (EU) 910/2014 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)	
(27) ~~This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an identified or identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data, it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for~~	AT (Comments): AT welcomes that the definition of 'personal data' is maintained. SE (Comments): Sweden is in favour of clarifying the definition of personal data and pursue discussions on an amended and updated definition of this notion, with due consideration to the need to ensure a strong protection of privacy as well as a simplified and coherent legal framework from a compliance perspective. Therefore, we are positive to continue discussions on this matter.

Presidency compromise text	Drafting suggestions and Comments
~~those third parties who have such means at their disposal. An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. In this respect the Court of Justice of the European Union has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council[1]. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria in an implementing act.~~ 1 ~~Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj)~~	
(27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable. The European Data Protection Board should support controllers by adopting guidelines assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to pseudonymise personal data effectively, and clarifying circumstances whether a natural	AT (Comments): • AT supports assigning the competence to issue guidelines regarding pseudonymisation and the identifiability of a natural person to the EDPB. • AT can support the proposed Recital 27a. ES (Comments):

Presidency compromise text	Drafting suggestions and Comments
person is identifiable and means reasonably likely to be used to identify a natural person, including means and criteria to determine whether data resulting from pseudonymisation may no longer constitute personal data for certain entities. While controllers remain fully responsible to determine whether data resulting from pseudonymisation is personal, the guidelines should support controllers in implementing such measures and criteria, and provide guidance to demonstrate whether pseudonymised data do not lead to re-identification of data subjects.	We agree to the proposed wording appearing as 27a replacing that of the strikethrough recital 27. SE (Comments): See comment above in relation to the deleted text.
~~(28) In order to assess whether research meets the conditions of scientific research for the purpose of this Regulation, account can be taken of elements such as methodological and systematic approach applied while conducting the research in the specific area. Research and technology development should be conducted in academic, industry and other settings, including small and medium-sized undertakings, (Article 179(2) TFEU) and should be always of a of high quality and should adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability).~~	AT (Comments): AT supports the deletion (in line with the deletion of the definition of "scientific research"). ES (Comments): On scientific research. It seems to us good to delete it as it is ambiguous and therefore gives rise to interpretative problems. We are in favour of opening up the concept of scientific research but using commonly accepted definitions such as the Frascati Manual (OECD, 1963) which describes R & D as *"creative and systematic work undertaken in order to increase the stock of knowledge-including knowledge of humankind, culture, and society-and to devise new applications of available knowledge"*.
(29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it ~~is not~~**should not be** necessary to ascertain on the basis of Article 6(4) of ~~this~~ Regulation **(EU) 2016/679** whether the purpose	AT (Comments): AT welcomes the additions to Recital 29. The explanations regarding the term 'scientific research' within the meaning of the GDPR provide greater clarity and legal certainty.

Presidency compromise text	Drafting suggestions and Comments
of the further processing is compatible with the purpose for which the personal data are initially collected. **Such further processing should be considered compatible, provided that it is carried out in compliance with the principle of purpose limitation and subject to appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89. The qualification of processing as being carried out for scientific research purposes should be based on objective characteristics of the research activity and should not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679. In order to assess whether scientific research activities meet the conditions of scientific research for the purpose of Regulation (EU) 2016/679, account can be taken of elements such as the purpose of the research, the methodological approach and ethical standards applied in the specific area while conducting the research, and adherence to the principles of transparency, reliability, accountability and oversight, verifiability, and rules for research integrity. Scientific research activities should concur to public interest and well-being, prevent individuals from being subjected to harm or other adverse effects due to participating in scientific research and include – among other things – the respect for human autonomy and the notion of consent to participate in research. Scientific research activities can, amongst others, support innovation such as technology development and may be conducted in academic, industry and other settings, by public authorities or private entities, including small and medium sized undertakings.**	ES (Comments): We consider the text to be correct. Support that further processing for scientific research should be considered compatible with primary treatment without necesity that the compatibility judgement of Art. 6.4 has to be applied. Also in favour of having to apply the safeguards of Art. 89. SE (Comments): SE is in favour of keeping the definition in 4.38.
(30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in various phases in the AI lifecycle, such as the training, testing and validation	AT (Comments): See previous AT comments/proposals

Presidency compromise text	Drafting suggestions and Comments
phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes of a legitimate interest within the meaning of Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.	
(31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller, appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.	AT (Comments): See previous AT comments/proposals

Presidency compromise text	Drafting suggestions and Comments
(32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research ~~therefore pursues a~~**may be necessary for the purposes of the** legitimate ~~interest~~**interests pursued by a controller or by a third-party** within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State **law. Scientific research can also follow public interest and be based on Member States and Union** law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.	AT (Comments): AT can support the proposed changes to Recital 32. ES (Comments): We support the COM proposal which seeks to provide researchers with legal certainty by validating the "legitimate interest" as a clear legal avenue provided that the conditions of Article 6.1 (f) are guaranteed that balance this legitimate interest with the rights and freedoms of natural persons.
(33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing. In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and remove special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate	AT (Comments): See previous AT comments/proposals ES (Drafting suggestions): *(33) the development of certain AI systems and models may involve the collection of large volumes of data, including personal data and special categories thereof. Special categories of personal data may exist residually in the training, testing or validation datasets, or may be retained in the AI*

Presidency compromise text	Drafting suggestions and Comments
measures during the entire lifecycle of an AI system or AI model and, once it identifies such data, effectively remove them. If removal would require disproportionate effort, notably where the removal of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, the controller should effectively protect such data from being used to infer outputs, being disclosed or otherwise made available to third parties. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679.	*system or model, even if the processing of such special categories is not necessary for the purpose of the processing.* ***While the development of AI systems and models can contribute to technological progress and social well-being, this should not undermine the protection of fundamental rights, in particular in the case of special categories of personal data requiring special protection, given their particular sensitivity and the risk of discrimination that their processing may entail.*** ***In order not to disproportionately hamper the development and functioning of AI, a derogation from the prohibition on processing special categories of personal data laid down in Article 9 (2) should be allowed. However, this derogation should be subject to strict safeguards ensuring that the residual treatment does not result in significant risks to the rights and freedoms of natural persons.*** *The derogation should only apply where the controller has effectively implemented appropriate organisational and technical measures to prevent the processing of such data and takes appropriate measures throughout the life cycle of the AI system or model.* ***Such measures may include automated filtering techniques at the data collection stage, sample reviews, special category detection mechanisms and, where technically feasible, state-of-the-art privacy protection techniques such as differential privacy or Federated learning****. 11 these data have been identified, they must be effectively deleted by the controller.* *If the deletion requires a disproportionate effort, in particular where the deletion of special categories of data stored in the AI system or model requires the complete re-engineering of the system or model in such a way*

Presidency compromise text	Drafting suggestions and Comments
	as to render its operation technically or economically impracticable, the controller should effectively protect that data. ***Such protection should effectively prevent their use to generate inferences about special categories concerning identified or identifiable persons, their disclosure or their making available to third parties****.* ***In accordance with the principle of accountability, the controller should establish a process of regular verification, assessment and assessment of the effectiveness of the measures implemented or when there are significant changes to the AI system or model. It should also Comprehensively document the measures taken, the results of the periodic evaluations and any findings, so that it can demonstrate compliance with the obligations laid down down in this Regulation.*** ***Given the sensitive nature of special categories of personal data and the high risk inherent in their processing in the context of the development and operation of AI systems and models, the controller should carry out a data protection impact assessment in accordance with Article 35. That assessment should specifically assess the risks arising from the residual processing of those categories of personal data****.* This exception should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In such a case, the controller should rely on one of the exceptions set out out out in points (a) to (j) of paragraph 2 of Article 9. ES (Comments):

Presidency compromise text	Drafting suggestions and Comments
	The current wording enables the processing of special categories of data in general in AI systems. We believe that the new 9.2.k deriving from this recital should exempt the processing of special categories of data when such processing has a 'residual' meaning that is difficult to avoid in practice. We therefore support the Commission's proposal. However, we think that if the processing of special categories of data is not residual, but is processed because the purpose requires it, then this new exception of 9.2.k should not be used but any of the existing ones (9.2.a to 9.2.j.).
(34) **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric data includes two distinct functions, namely the identification of a natural person or the verification (also called authentication) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary **and proportionate** for a purpose pursued by the controller~~,~~ and **when provided for under Union or Member States law. The controller should choose from equally effective means the less intrusive one. This derogation should apply where** suitable safeguards apply to ~~enable the data subject to have sole control of~~**ensure that the biometric data or the means needed for** the verification ~~process~~**are under the sole control and possession of the data subject**. For example, **this is**	AT (Drafting suggestions): (34) **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric data includes two distinct functions, namely the identification of a natural person or the verification (also called authentication) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary **and proportionate** for a purpose pursued by the controller~~,~~ and **when provided for under Union or Member States law. The controller should choose from equally effective means the less intrusive one. This derogation should apply where** suitable safeguards apply to ~~enable the data subject to have sole control of~~**ensure that the**

Presidency compromise text	Drafting suggestions and Comments
the case where the biometric data are securely stored solely at the ~~side~~**device** of the data subject or are securely stored ~~at the side of~~**by** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, ~~that~~**and subject to measures ensuring the overall security of** processing ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~**, including during the enrolment phase of data subject's** biometric data ~~or only for a very limited time~~**and** during the verification process.	**biometric data or the means needed for** the verification ~~process~~**are under the sole control and possession of the data subject**. For example, **this is the case** where the biometric data are securely stored solely at the ~~side~~**device** of the data subject or are securely stored ~~at the side of~~**by** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, ~~that~~**and subject to measures ensuring the overall security of** processing ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~**, including during the enrolment phase of data subject's** biometric data ~~or only for a very limited time~~**and** during the verification process. **<u>This could be the case where [describe practical use cases]</u>.** AT (Comments): AT can support the amendments. In addition, practical examples / use cases should be added at the end of this Recital. ES (Drafting suggestions): We propose the following wording of this recital, as well as the corresponding wording of Article 9.2 (l). *(34) Biometric data, as defined in Article 4, point (14), of Regulation (EU) 2016/679, involve the processing of certain characteristics of a natural person by specific technical means that enable or confirm the unique identification of that person.* *The concept of biometric data comprises two distinct functions, namely the identification of a natural person or the verification, also referred to as authentication, of his or her declared identity, which are based on different technical processes. The identification process is based on a 'one-to-many'*

Presidency compromise text	Drafting suggestions and Comments
	search of the biometric data of the data subject in a database, while the verification process is based on a 'one-to-one' comparison of the biometric data provided by the data subject, thereby declaring his or her identity. *An exception to the prohibition on processing biometric data laid down in Article 9 (1) of the Regulation should be allowed where verification of the declared identity of the data subject is necessary for a purpose pursued by the controller, and appropriate safeguards are in place allowing the data subject to have sole control of the verification process. Exclusive* ***control means that the data subject can effectively decide when and how his or her biometric data are used for verification, without the controller having the technical capacity to access such biometric data in decrypted form or process them outside the strictly limited comparison process necessary for verification. This can be achieved, for example, when biometric data are stored securely on the device of the data subject under his or her physical possession, or in a system of the controller, but in encrypted format with robust state-of-the-art cryptographic techniques, and the encryption key or equivalent means are under the sole control of the data subject, so that the controller cannot decrypt them without the active intervention of the data subject****. In such cases, the processing is not likely to result in significant risks to the fundamental rights and freedoms of the data subject* ***In order to ensure the effective protection of the rights of the data subject, the controller should implement appropriate technical and organisational measures. Those measures should include, inter alia, procedures allowing the data subject to Revoke at any time his or her biometric identifiers, the use of robust and up-to-date cryptographic algorithms, technical controls preventing access to biometric templates without the key under the control of the data subject, as well as as as the processing of biometric data***

Presidency compromise text	Drafting suggestions and Comments
	exclusively locally, without clear data transmission or synchronisation with centralised systems, except where strictly necessary for verification and with appropriate safeguards. ***Specific safeguards should also be established at the initial stage of registration, during which the biometric data of the data subject are captured and stored for the first time, so that the data subject retains effective control from the beginning of the processing.*** ES (Comments): We find well the COM's initial proposal leading to the new 9.2.l GDPR that exempts the use of biometrics in one-to-one cases (authentication) and when templates or encryption means are under the sole control of the user. We do not support the addition here of making this exception conditional on there being legal protection in national or Union rules, as it leaves this COM proposal in no way. Nor does the addition *of "The controller should choose from equally effective means the less intrusive one*" introduce uncertainty for the controller, which is understood as effectiv. What seems needed to be done is an impact assessment that includes a proportionality assessment that evaluates the necessity, appropriateness and proportionality, and on this there is CJEU case-law that gives legal certainty. In favour of safety add-ons. SE (Comments): See Sweden's comment below in relation to the proposed amendment in Article 9(2)(l) of the GDPR.

Presidency compromise text	Drafting suggestions and Comments
(35) Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain **confirmation** from the controller ~~confirmation~~ as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. ~~By contrast, it should be clarified in~~ Article 12 **(5) of that** ~~of the~~ Regulation **already provides that where the request to exercise** ~~that~~ the right of access~~, which is from the outset favourable to data subjects,~~ **is manifestly unfounded or excessive, the controller may either charge a reasonable fee or refuse to act on the request. It is important to clarify that this** should ~~not be abused in the sense that~~**apply also where an abusive intention on the part of** the data ~~subjects abuse them for purposes other than the protection of their data~~**subject submitting those requests can be demonstrated by the controller**. For example, such an ~~abuse of the right of access~~**abusive intention** would arise where the data subject ~~intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make~~**submits** excessive ~~use of the right of access~~**numbers of identical or largely similar requests** with the ~~only~~**sole** intent of causing damage or harm to the controller**. Another example of abusive intention includes situations** ~~or~~ when an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller. ~~Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of proof regarding the excessive character of a request than regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character of a request concerns the possibly abusive conduct of a data subject, which lies primarily outside the controller's sphere of influence,~~	AT (Drafting suggestions): (35) **Chapter III of of Regulation (EU) 2016/679 sets out rights of the data subject and corresponding obligations of the controller. Inter alia,** Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain **confirmation** from the controller ~~confirmation~~ as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. ~~By contrast, it should be clarified in~~ Article 12 **(5) of that** ~~of the~~ Regulation **already provides that where the request to exercise a right of the data subject** ~~that~~ **~~the right of access~~**~~, which is from the outset favourable to data subjects,~~ **is manifestly unfounded or excessive, the controller may either charge a reasonable fee or refuse to act on the request. It is important to clarify that this** should ~~not be abused in the sense that~~**apply also where an abusive intention on the part of** the data ~~subjects abuse them for purposes other than the protection of their data~~**subject submitting those requests can be demonstrated by the controller**. For example, such an ~~abuse of the right of access~~**abusive intention** would arise where the data subject ~~intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make~~**submits** excessive ~~use of the right of access~~**numbers of identical or largely similar requests** with the ~~only~~**sole** intent of causing damage or harm to the controller**. Another example of abusive intention includes situations** ~~or~~ when an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller. ~~Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of proof regarding the excessive character of a request than~~

Presidency compromise text	Drafting suggestions and Comments
~~and therefore the controller may be able to prove such abuse only to a reasonable level. In any event, while requesting access under Article 15 of Regulation (EU) 2016/679 the data subject should be as specific as possible. Overly broad and undifferentiated requests should also be regarded as excessive.~~	~~regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character of a request concerns the possibly abusive conduct of a data subject, which lies primarily outside the controller's sphere of influence, and therefore the controller may be able to prove such abuse only to a reasonable level. In any event, while requesting access under Article 15 of Regulation (EU) 2016/679 the data subject should be as specific as possible. Overly broad and undifferentiated requests should also be regarded as excessive.~~ AT (Comments): • AT welcomes the clarifications in Recital 35. • However, the extended excessiveness clause should apply to all rights of the data subject. It is not clear why an abusive intention can only be relevant with regard to the right of access, but not with regard other rights of the data subject. ES (Comments): Although we do not have a proposal for an alternative wording for this recital, we consider that it should be revised. In fact, we propose an improved wording for 12.5. (*see article below*) SE (Comments): To Sweden, it is essential to ensure that proposed amendment corresponds to need of controllers while safeguarding an effective protection on behalf of the data subjects. It should be considered whether the deletion of a lower

Presidency compromise text	Drafting suggestions and Comments
	burden of proof in this regard could risk of hindering a real alleviation on behalf of the controllers.
	AT (Drafting suggestions): **(35a) Article 57 of Regulation (EU) 2016/679 provides rules for situations where requests from a data subject to the supervisory authority, including complaints under Article 77 of Regulation (EU) 2016/679, are manifestly unfounded or excessive, in particular because of their repetitive character. Articles 12 and 57 of Regulation (EU) 2016/679 use the same wording and pursue the same objective, namely to provide for an exception to the free-of-charge principle applicable to the tasks carried out by the supervisory authorities and the exercise of rights of the data subject, respectively. In order to reduce the burden of controllers with regard to excessive requests, which may also occur in relation to requests, including complaints, to the supervisory authority concerning the controller, the notion of excessivity in Article 57 of Regulation (EU) 2016/679 should be adapted likewise.** AT (Comments): • new Recital relating to the proposed amendment of Article 57(4) in order to align it with Article 12(5) • second sentence reflects opinion of Attorney General in CJEU case C-526/24 (subject to outcome of the case)
(36) Article 13 of Regulation (EU) 2016/679 requires the data controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of data	AT (Drafting suggestions): (36) Article 13 of Regulation (EU) 2016/679 requires the data controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that

Presidency compromise text	Drafting suggestions and Comments
controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of ~~the~~**that** Regulation, this derogation should be extended to situations where the processing is not likely to result in a high risk, within the meaning of Article 35 of ~~the~~**that** Regulation, and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 **of Article 13** in the light of the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller. **The application of the derogation from the information obligation should not undermine the principle of transparency and should be limited to situations where the controller can objectively demonstrate that the data subject already possesses the required information.** These should be the situations where the **personal data are collected in the** context of ~~the~~**a direct, limited and clearly circumscribed** relationship between ~~the~~**data subjects and a** controller and ~~the data subject is very clear and circumscribed and the controller's activity is not data-intensive~~**does not involve the processing of a large amount of personal data**, such as the relationship between a craftsman and their clients, where the scope of processing is limited to the minimum data necessary to perform the service~~. The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment. In such circumstances, that is to say when the processing is non data-intensive, non-complex and where the controller collects a low amount of personal data, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller as well as on the purpose of the processing when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679~~. The same should apply to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members	provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of data controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of ~~the~~**that** Regulation, this derogation should be extended to situations where the processing is not likely to result in a high risk, within the meaning of Article 35 of ~~the~~**that** Regulation, and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 **of Article 13** in the light of the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller. **The application of the derogation from the information obligation should not undermine the principle of transparency and should be limited to situations where the controller can objectively demonstrate that the data subject already possesses the required information.** These should be the situations where the **personal data are collected in the** context of ~~the~~**a direct, limited and clearly circumscribed** relationship between ~~the~~**data subjects and a** controller and ~~the data subject is very clear and circumscribed and the controller's activity is not data-intensive~~**does not involve ~~the~~ large scale processing ~~of a large amount~~ of personal data**, such as the relationship between a craftsman and their clients, where the scope of processing is limited to the minimum data necessary to perform the service~~. The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment. In such circumstances, that is to say when the processing is non data-intensive, non-complex and where the controller collects a low amount of personal data, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller as well as on the purpose of the processing when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the~~

Presidency compromise text	Drafting suggestions and Comments
and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information.	~~requirements laid down in Regulation (EU) 2016/679~~. The same should apply to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information. AT (Comments): • AT can support the compromise proposal on Article 13(4) and Recital 36 GDPR. The proposed amendments provide important clarifications. • For further clarification, “large scale processing of personal data” could be used (instead of „processing of large amounts of personal data“). That term is also used in other GDPR provisions and covered in EDPB guidelines. ES (Drafting suggestions): *[...] The activity of the controller does not require intensive use of data when it collects a small amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment* ***or in relations with public authorities or public bodies or private entities for the performance of a task in the public interest****. ...’*

Presidency compromise text	Drafting suggestions and Comments
	ES (Comments): We support the initial COM proposal with the addition of wording suggested here in bold on the COM proposal. (*see also the proposed alternative wording of Article 13 (4).* SE (Comments): The introduction of requiring the controller to objectively demonstrate that the data subject already possesses the information could be reconsidered as it may counteract the ambition to ease the administrative burdens from a compliance perspective.
(37) Where the **further** processing **by the same controller** takes place for the purpose of scientific research and the provision of information to the data subject proves to be impossible or would involve a disproportionate effort it should not be necessary to provide the information provided for under Article 13 of this Regulation. The controller should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort. The provision of the information would involve a disproportionate effort in particular where the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects. In such situations the controller should inform data subjects indirectly, such as by making the information publicly available. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information	ES (Comments): . SE (Comments): The practical implications as regards the proposed limitation to “further processing by the same controller” needs to be further discussed in order to ensure that this derogation corresponds to the needs and objectives pursued.

Presidency compromise text	Drafting suggestions and Comments
publicly available should be determined depending on the context of the research project and the data subjects involved.	
~~(38) Article 22 of Regulation (EU) 2016/679 provides for rules governing the processing of personal data when the data controller makes decisions which have legal effects or similarly significant effects on the data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified that decisions based solely on automated processing are allowed when specific conditions are met, as set out in Regulation (EU) 2016/679. It should also be clarified that when assessing whether a decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. This means that the fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing When several equally effective automated processing solutions exist, the controller should use the less intrusive one.~~	AT (Comments): AT can support the proposed deletion of the amendment to Article 22 GDPR. ES (Drafting suggestions): Our proposal for Art. 22 is as follows: *'1. A decision which produces legal effects concerning a data subject or similarly significantly affects him or her may be based solely or substantially on automated processing, including profiling.* *2. In the cases referred to in paragraph 1, the controller shall ensure at least the right of the data subject to obtain human intervention, to express his or her point of view, to challenge the decision and the right to explicability of the automated decision, which shall include access to clear, comprehensible and meaningful information on the criteria, determining factors and merits of the decision as well as on its consequences for the data subject.* *3. Where the decisions referred to in paragraph 1 are taken through the use of artificial intelligence systems, the controller shall take into account the nature and level of risk of the system for the purposes of implementing the safeguards provided for in this Article.'* ES (Comments):

Presidency compromise text	Drafting suggestions and Comments
	We are in favour of amending Article 22 on automated decision-making. *See the proposal below in the articles*. We are therefore not in favour of deleting this recital, although it should be brought into line with the text we are proposing
(39) In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation. In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should ~~prepare~~**establish and make public** a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person~~. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption~~**, as well as a common list of circumstances in which a personal data breach does not result in such a high risk**. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the	AT (Drafting suggestions): (39) In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should ~~**be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation**~~ **refer to an "impactful risk" ["relevant risk"/"increased risk"]**. In the case of a data breach that is not likely to result in ~~**a high risk**~~ **an "impactful risk" ["relevant risk"/"increased risk"]** to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should ~~prepare~~**establish and make public** a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in ~~**a high risk**~~ **an "impactful risk" ["relevant risk"/"increased risk"]** to the rights and freedoms of a natural person~~. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption~~**, as well as a common list of**

Presidency compromise text	Drafting suggestions and Comments
obligations of controllers to notify those breaches. **The alignment of notification thresholds does not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) and Article 30 of Regulation (EU) 2016/679.**	**circumstances in which a personal data breach does not result in such ~~a high risk~~ an "impactful risk" ["relevant risk"/"increased risk"]**. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in **~~a high risk~~ an "impactful risk" ["relevant risk"/"increased risk"]** to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. **The ~~alignment~~ amendment of the notification thresholds does not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) and Article 30 of Regulation (EU) 2016/679.** AT (Comments): • AT remains sceptical about raising the threshold for data breach notifications to the supervisory authority. • A possible compromise could be to use a threshold between "risk" and "high risk", such as "impactful risk", "relevant risk", "increased risk" or likewise ES (Comments): see the outcome document on the 'single entry point' SE (Comments): See comments below in relation to Article 33.

Presidency compromise text	Drafting suggestions and Comments
(40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be ~~prepared~~**established and made public** by the Board ~~and adopted by the Commission as an implementing act~~. In order to facilitate compliance by controllers, the Board should also ~~prepare~~**establish and make public** a common template and a common methodology for conducting data protection impact assessments~~, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption~~. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary.	ES (Comments): We support the changes made to the COM proposal. We support that both lists are made and updated by the Board and do not need to be adopted by the COM. SE (Comments): See comments below in relation to article 35.
(41) Regulation (EU) 2018/1725 of the European Parliament and of the Council[2] applies to the processing of personal data by the Union institutions,	

Presidency compromise text	Drafting suggestions and Comments
bodies, offices and agencies. Directive (EU) 2016/680 of the European Parliament and of the Council[3] applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Regulation (EU) 2018/1725 and Directive (EU) 2016/680 should be brough into alignment with the amendments to Regulation (EU) 2016/679 introduced by this Regulation. 2 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj). 3 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).	
(42) As clarified in recital 5 of Regulation (EU) 2018/1725, whenever the provisions of Regulation (EU) 2018/1725 follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union, be interpreted homogeneously. The scheme of Regulation (EU) 2018/1725 should be understood as equivalent to the scheme of Regulation (EU) 2016/679. Therefore, this Regulation also amends the provisions of Regulation (EU) 2018/1725 that are concerned by the amendments of	

Presidency compromise text	Drafting suggestions and Comments
Regulation (EU) 2016/679, insofar as the latter amendments are also relevant in the context of the processing of personal data by the Union institutions, bodies, offices and agencies.	
(43) In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Directive (EU) 2016/680 and any other Union legal act applicable to such processing of personal data should follow after the adoption of this regulation, in order to allow for their application as close as possible to the entry into application of the amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.	
(44) The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely Regulation (EU) 2016/679, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person. The amendments presented in this Regulation continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. The relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.	AT (Comments): See previous AT comments/proposals
The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment should continue to be allowed only on the basis of consent. Similar to the approach in Directive 2002/58/EC, this	

Presidency compromise text	Drafting suggestions and Comments
requirement should not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, when that is based on Union or Member State law within the meaning of Article 6 of Regulation (EU) 2016/679 and if it fulfils all conditions of lawfulness laid down in that provision, and is done for the objectives laid down in Article 23(1) of Regulation (EU) 2016/679.	
With a view to reducing the compliance burden and providing legal clarity to controllers, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by the data subject, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, this Regulation should therefore provide that the processing is lawful. The controller, such as a media service provider, may mandate a processor, such as a market research company, to carry out the processing on its behalf.	
For the subsequent processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied. It is the responsibility of the controller in the light of the principle of accountability to choose the appropriate legal basis for the intended processing. In order to be able to rely on legitimate interest under Article 6(1), point f, of Regulation (EU) 2016/679 as a ground for the subsequent processing of personal data, the controller must show that it pursues the controller's or third parties' legitimate interest, the processing is necessary in order to achieve the purpose of that legitimate interest, and the interests or fundamental rights of the data subject do not override the interests pursued by the controller. In this context,	

Presidency compromise text	Drafting suggestions and Comments
controllers should take outmost account of the following elements: whether the data subject is a child; the reasonable expectations of data subject; the impact on the individual either because of the scale of data processed or the sensitivity of the data processed; the scale of the processing at issue in the sense that the processing cannot be particularly extensive either because of their amount or the range of categories of data; the processing should be based on data limited to what is necessary and cannot be based on monitoring of large parts of the online activity of the data subjects; and other relevant factors as appropriate. The processing should not give rise to the continuous monitoring of the data subject's private life.	
Where the controller cannot rely on legitimate interest as a legal ground for the subsequent processing, the processing should be based on another ground in Article 6(1), in particular on consent in accordance with Articles 6 and 7 of Regulation (EU) 2016/679, provided that all principles of Regulation (EU) 2016/679 are met.	
(45) Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the data subjects which may consent just in order to avoid repeating requests. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period.	AT (Comments): See previous AT comments/proposals ES (Comments): .
(46) Data subjects should have the possibility to rely on automated and machine-readable indications of their choice to consent or refuse a consent request or object to the processing of data. Such means should follow the state of the art. They can be implemented in the settings of a web browser or	AT (Comments): See previous AT comments/proposals

Presidency compromise text	Drafting suggestions and Comments
in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation should support the emergence of market-driven solutions with appropriate interfaces. The controller should be obliged to respect automated and machine-readable indications of data subject's choices once there are available standards. In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices. The obligation for providers of web browsers to provide the technical means for data subjects to make choices with respect to the processing should not undermine the possibility for media service providers to request consent by data subjects.	ES (Comments): We do not agree that the media are not obliged to respect the choice of the person concerned.
(47) Directive 2002/58/EC on privacy and electronic communications 'ePrivacy Directive'), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of user's or subscriber's terminal equipment used for such communications. The current provision of Article 5(3) of Directive 2002/58/EC should remain applicable insofar as the subscriber or user is not a natural person, and the information stored or accessed does not constitute or lead to the processing of personal data.	AT (Comments): See previous AT comments/proposals
(48) Article 4 of Directive 2002/58/EC should be repealed. Article 4 of Directive 2002/58/EC sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements. Subsequently, Directive (EU) 2022/2555 has set new requirements as regards cybersecurity risk-management measures and incident reporting for those providers. In order to	

Presidency compromise text	Drafting suggestions and Comments
reduce overlapping obligations for entities in the electronic communications sector, Article 4 of Directive 2002/58/EC should be repealed. As regards the security of processing of personal data pursuant to Article 4(1) and (1a) of this directive and the notification of personal data breaches pursuant to Article 4(3) to (5) of Directive 2002/58/EC this directive, the Regulation (EU) 2016/679 already provide for comprehensive and up-to-date rules. These rules should therefore apply to providers of publicly available electronic communication services and providers of public communications networks, thereby ensuring that one regime applies to the controllers and processors.	
(58) The European Data Protection Supervisor ~~was~~**and the European Data Protection Board were** consulted in accordance with Article ~~42(1)~~**42** of Regulation (EU) 2018/1725 of the European Parliament and of the Council[4], and delivered ~~its~~**their joint** opinion on ~~[DATE]. The European Data Protection Board was consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on [DATE]~~**10 February 2026**. 4 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).	
(59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU)	AT (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
2022/2065 and Regulation (EU) 2022/1925 provide a comprehensive regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that the objectives and material provisions of the Platform-to-Business Regulation are largely covered by the Digital Services Act and the Digital Markets Act, Regulation (EU) ~~2019/1050~~**2019/1150** should be repealed. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty **and for purposes of keeping the necessary level of protection for business users**, selected definitions in Article 2, the provisions on restrictions and suspensions in Article 4, as well as on the internal complaint-handling system in Article 11 of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, **or that are not covered by other legal acts,** in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and Article 15 ensuring enforcement, will temporarily remain in application until ~~the original acts are amended.~~**2032.**	(59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 provide a ~~comprehensive~~ regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that **some** objectives and material provisions of the Platform-to-Business Regulation are ~~largely~~ covered by the Digital Services Act and the Digital Markets Act, **certain provisions of** Regulation (EU) ~~2019/1050~~**2019/1150** should be repealed. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty **and for purposes of keeping the necessary level of protection for business users**, ~~selected definitions in~~ **Articles 2, points (1) to (10) and (13), 3, 4, 5, 7, 10, 11 and 15 should remain in application as they contain obligations that are not fully covered by Regulations (EU) 2022/2065 and (EU) 2022/1925.** ~~the provisions on restrictions and suspensions in Article 4, as well as on the internal complaint-handling system in Article 11 of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, **or that are not covered by other legal acts,** in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and Article 15 ensuring enforcement, will temporarily remain in application until the original acts are amended.~~**2032.** AT (Comments):

Presidency compromise text	Drafting suggestions and Comments
	AT: While AT acknowledges and supports the Commission's efforts to reduce administrative burdens by avoiding potential overlaps between the P2B Regulation and other EU legislation, we do not agree with the approach of repealing the P2B Regulation in general and refer to our comments on Article 10 (see below) and our non-paper with other Member States. Regarding the changes made in the recital 59 we agree that Articles 4 and 11 of the P2B-Regulation should be retained not only because of cross-references in other legal acts, but as a matter of principle, since they are not covered by other legal acts (esp. DMA and DSA). Their repeal would lead to a reduction in the level of protection for business users and they must therefore be retained. ES (Comments): no position yet SE (Comments): As previously stated, SE is in favour of proposals that reduce the administrative burden on businesses by avoiding potential overlaps between Regulation 2019/1150 and other EU legislation. It must however be ensured that the repeal of Regulation 2019/1150 does not result in ambiguity for companies and that no gaps arise in the legislation, especially for SMEs. SE are therefore in favour of the drafting suggestions put forward by BE on recital 59 and article 10.

Presidency compromise text	Drafting suggestions and Comments
(61) The amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 are based on Article 16 TFEU. The amendments to Directive 2002/58/EC are based on Article 16 TFEU and Article 114 TFEU. All other amendments are based on Article 114 TFEU.	
Article 3 **Amendments to Regulation (EU) 2016/679 (GDPR)**	
Regulation (EU) 2016/679 is amended as follows:	
1. Article 4 is amended as follows:	
~~(a) in point 1, the following sentences are added:~~	
~~'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'~~	AT (Comments): AT welcomes that the definition of 'personal data' remains unchanged. ES (Drafting suggestions): *'Article X. Identification, anonymisation and transmission of data* *1.Where information which the controller processes or communicates on the premise that it does not make it possible to identify the natural person is communicated to third parties, the controller shall make a prior and documented*

Presidency compromise text	Drafting suggestions and Comments
	assessment of whether, in the joint and functional context of processing operations, any of the recipients or related subjects, including processors, has or may reasonably have the means to identify the natural person. In that case, such information shall be considered as personal data for the purposes of this Regulation. *2. Information shall be considered personal data where the lack of identifiability results mainly from an artificial fragmentation of the processing, the use of apparent intermediaries or an organisational or contractual separation which, as a whole, reasonably enables or facilitates the identification of the natural person.* *3. Information shall again be considered to be personal data for the purposes of this Regulation where, as a result of technical, organisational, structural or legal changes, one of the subjects involved in the processing has, or may reasonably have, the means to identify the natural person.'* ES (Comments): We support the COM's proposal to amend the definition of personal data, although we believe that the definition it proposes is lacking. We therefore propose the following wording: LV (Comments): LV proposes that this point be included in the recitals of the GDPR in order to ensure the uniform application of the legal norm across the Member States. SE (Comments):

Presidency compromise text	Drafting suggestions and Comments
	Sweden is in favour of clarifying the definition of personal data and pursue discussions on an amended and updated definition of this notion, with due consideration to the need to ensure a strong protection of privacy as well as a simplified and coherent legal framework from a compliance perspective. Therefore, we are positive to continue discussions on this matter.
(b) the following points are added:	
'(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;	AT (Comments): See previous AT comments/proposals
(33) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;	AT (Comments): See previous AT comments/proposals
(34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;	AT (Comments): See previous AT comments/proposals
(35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;	AT (Comments): See previous AT comments/proposals

Presidency compromise text	Drafting suggestions and Comments
(36) 'media service provider' means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;'	AT (Comments): See previous AT comments/proposals
(37) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.'	AT (Comments): See previous AT comments/proposals
~~(38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'~~	AT (Comments): AT supports that no definition of "scientific research" is included. ES (Comments): We feel it is good to delete the definition proposed by the COM as it is ambiguous and therefore gives rise to problems of interpretation. We are in favour of opening up the concept of scientific research but using commonly accepted definitions such as the Frascati Manual (OECD, 1963) which describes R & D as *"creative and systematic work undertaken in order to increase the stock of knowledge-including knowledge of humankind, culture, and society-and to devise new applications of available knowledge"*. LV (Drafting suggestions): "scientific research" means any research **carried out with the aim of generating new scientific insights, complementing existing knowledge or applying it in novel ways, in the public interest.**

Presidency compromise text	Drafting suggestions and Comments
	LV (Comments): The EDPB and the EDPS, as well as several Member State delegations, have supported the introduction of a common definition of 'scientific research' in the GDPR. Therefore, LV proposes that the definition of ''scientific research'' be retained and that the discussion on it be continued. LV emphasises that the primary purpose of scientific research should be oriented towards the public interest. Explanatory information clarifying that technological development may be regarded as being in the public interest, as well as the need to observe the relevant ethical standards in the relevant research area, should be set out in the recitals (29) of the GDPR. SE (Drafting suggestions): 38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.' SE (Comments): SE is in favour of introducing a definition of scientific research, as introduced in the Commission's proposal.

Presidency compromise text	Drafting suggestions and Comments
2. Article 5 (1)(b) is replaced by the following:	ES (Comments): In favour of the current wording. We consider it correct that the further processing for scientific research is considered compatible with the primary treatment and therefore need that the compatibility judgement of Art. 6.4 has to be applied. Also in favour of having to apply the safeguards of Art. 89 (1).
'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, **subject to the application of appropriate safeguards** in accordance with Article 89(1), be considered to be compatible with the initial ~~purposes, independent of the conditions of Article 6(4) of this Regulation,~~**purpose** ('purpose limitation');'	AT (Comments): • Provided that the definition for „scientific research" is deleted, AT can support the compromise proposal • AT understands the reference "subject to the application of appropriate safeguards in accordance with Article 89(1)" as clarification of the current legal situation. • Such clarification could also be made in other provisions referring to Art 89(1) GDPR, in particular Article 9(2)(j) and Article 17(3)(d) GDPR LV (Drafting suggestions): ''b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. ~~further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to the application of appropriate safeguards in accordance with Article 89(1), be considered to be compatible with the initial purpose ('purpose limitation');~~''' LV

Presidency compromise text	Drafting suggestions and Comments
	(Comments): LV supports the clarification that further processing for scientific research purposes should be considered compatible with the original purpose, subject to appropriate safeguards under Article 89(1). LV suggests that the provision stating that '' *further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to the application of appropriate safeguards in accordance with Article 89(1), be considered to be compatible with the initial purpose ('purpose limitation'),*'' be moved to the recitals of the GDPR.
3. Article 9 is amended as follows:	ES (Comments): The current wording enables the processing of special categories of data in general in AI systems. We believe that the new 9.2.k should exempt the processing of special categories of data when such processing has a 'residual' meaning that is difficult to avoid in practice. We think that if the processing of special categories of data is not residual, but is processed because the purpose requires it, then this new exception of 9.2.k should not be used but any of the existing ones (9.2.a to 9.2.j.
(a) in paragraph 2, the following points are added:	
'(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5.	AT (Comments): See previous AT comments/proposals ES

Presidency compromise text	Drafting suggestions and Comments
	(Drafting suggestions): We therefore propose the following wording for 9.2.k: *9.2.k) the processing in the context of the development and operation of an AI system, as defined in Article 3, point (1), of Regulation (EU) 2024/1689, or of an AI model, subject to the conditions referred to in paragraph 5,* ***unless such personal data are necessary for the purpose of the processing. In the latter case, the controller shall rely on one of the exceptions set out out out in points (a) to (j) of this paragraph.*** LV (Comments): LV recalls that Article 9(1) of GDPR establishes a general prohibition on the processing of special categories of personal data, and that the circumstances under which such processing may be permitted are exhaustively enumerated in Article 9(2). In this context, LV expresses concern regarding the proposed expansion of the derogations allowing the processing of special categories of personal data for the purposes of the development and operation of an AI system. LV notes, in particular, that introducing a sector- specific derogation limited to a single technological domain risks undermining the principle of technological neutrality inherent in GDPR and may give rise to legal fragmentation. Latvia further observes that such an approach would, in effect, constitute a substantive and far- reaching derogation from the prohibition laid down in Article 9(1), and could be incompatible with the heightened level of protection for sensitive categories of personal data as established in the case- law of the Court of Justice of the European Union. LV therefore calls for continued and thorough deliberation on this proposed amendment, including a comprehensive assessment of its potential implications for the protection of fundamental rights. LV underlines that the proposed amendment appears to

Presidency compromise text	Drafting suggestions and Comments
	exceed the scope of a ‘’targeted amendments’’ and should accordingly be subject to a more detailed examination. SE (Comments): Sweden supports the proposed exemption for residual processing of special categories of personal data for development and operation of an AI system or an AI model set out in Article 9(2)(k) and 9(5). However, Sweden considers that the proposed provisions could benefit from further substantial discussions in order to fully enhance the aspects thereof, such as the notion of residual data, what aspects to consider in order to determine if a removal constitutes disproportionate efforts or the conception of effectively protecting such data from being disclosed
(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the **one-to-one** verification is under the sole control **and possession** of the data subject~~.~~ **and in so far as it is authorised by Union or Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject’**	AT (Comments): AT can support the compromise proposal ES (Drafting suggestions): *9.2.l. the processing of biometric data is necessary to confirm the identity of the data subject (verification), where the biometric data or the means necessary for verification are under the sole control of the data subject* ***and appropriate technical and organisational measures are put in place to protect his or her rights and freedoms****.* ES (Comments):

Presidency compromise text	Drafting suggestions and Comments
	We do not support the current wording at all. We support the COM proposal with some additions to provide greater legal certainty. We therefore propose an alternative wording to Article 9.2 (l) and the corresponding recital (34). LV (Comments): LV supports the Presidency's proposed compromise text. SE (Comments): As regards, the addition of "and possession", Sweden wonders whether this addition could exclude biometric verification in a situation where the means necessary "are securely stored at the side of the controller in a state-of-the-art encrypted form" (c.f. recital 34). If so, the reason for the addition should be further elaborated. Sweden considers that the addition of "in so far as it is authorised by Union or Member State law providing for appropriate safeguards" risks of causing a fragmented application within the internal market.
(b) the following paragraph is added:	
'5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller	AT (Comments): See previous AT comments/proposals ES (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.'	*5. For the processing referred to in paragraph 2, point (k):* *(a) Appropriate organisational and technical measures shall be implemented to prevent the collection and processing of special categories of personal data. If, despite the application of those measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation, or in the AI system or model, it shall delete those data. If the deletion requires a disproportionate effort, the controller shall effectively protect such data by preventing the results generated by the AI system or model from* ***disclosing special categories relating to identified or identifiable persons****, as well as their disclosure or making available to third parties.* ***The controller shall establish a process of regular verification, assessment and assessment of the effectiveness of the measures implemented and shall Comprehensively document those measures and the results of the assessments throughout the life cycle of the AI system or model.*** ***The controller shall carry out out a data protection impact assessment in accordance with Article 35, which shall include an assessment of the risks arising from the residual processing of special categories of data****.000* LV (Drafting suggestions): For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data t**hat are incidentally involved** in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires

Presidency compromise text	Drafting suggestions and Comments
	disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties. LV (Comments): LV considers it essential to underline that the exemption shall apply only to data that are incidentally included in the processing, and not to any intentional collection of such data.
4. In Article 12, paragraph 5 is replaced by the following:	
'5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character ~~or also, for~~**and, in the case of** requests under Article 15**, where an abusive intention on the part of** ~~because~~ the data subject ~~abuses the rights conferred by this regulation for purposes other than the protection of their data~~**submitting those requests can be demonstrated**, the controller may either:	AT (Drafting suggestions): '5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character ~~or also, for~~**and, in the case of requests under Article 15, or where an abusive intention on the part of** ~~because~~ the data subject ~~abuses the rights conferred by this regulation for purposes other than the protection of their data~~**submitting those requests can be demonstrated**, the controller may either: AT (Comments): • In principle, AT can support the compromise proposal. • However, the extended excessiveness clause should apply to all rights of the data subject. It is not clear why an abusive intention can only be relevant

Presidency compromise text	Drafting suggestions and Comments
	with regard to the right of access, but not with regard other rights of the data subject. ES (Drafting suggestions): We propose the following alternative wording: *Information provided under Articles 13 and 14, as well as any communication and any action taken under Articles 15 to 22 and 34, shall be provided free of charge.* *However, where requests made by a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, or where, in the case of requests based on Article 15, it appears objectively and manifestly that their exercise has no reasonable connection with the purposes of the right of access in relation to the protection of personal data, the controller may:* LV (Comments): LV supports the Presidency's proposed compromise text.
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or	ES (Drafting suggestions): *a) charge a reasonable fee, proportionate to the administrative costs of providing the information or taking the action requested; or*

Presidency compromise text	Drafting suggestions and Comments
(b) refuse to act on the request.	ES (Drafting suggestions): *b) refuse to act on the request, giving adequate reasons.*
The controller shall bear the burden of demonstrating that the request is manifestly unfounded or ~~that there are reasonable grounds to believe that it is~~ excessive**, or that the request is submitted with an abusive intention**.'	ES (Drafting suggestions): *The exercise of the rights provided for in Articles 15 to 22 shall not be subject to the obligation of the person concerned to give reasons for his or her request. However, the complete absence of any indication as to the purpose of the access may be taken into account together with the other relevant circumstances in order to assess whether the request is manifestly unfounded or excessive.* *The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.* LV (Comments): LV supports the Presidency's proposed compromise text. SE (Comments): See comment above in relation to recital 35.
5. In Article 13, paragraph 4 is replaced by the following:	

Presidency compromise text	Drafting suggestions and Comments
‘4. Paragraphs 1, 2 and 3 shall not apply where **and insofar as the data subject has the information and where** the personal data ~~have been~~**are** collected in the context of a ~~clear and~~**direct, limited and clearly** circumscribed relationship between data subjects and a controller exercising an activity that is not ~~data-intensive~~**likely to result in a high risk to the rights and freedoms of data subjects nor involve the processing of large amounts of personal data, special categories of personal data or complex processing operations** and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1~~, unless~~**.** **The first subparagraph shall not apply where** the controller **intends to process the data collected from the data subject for other purposes,** transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.’	AT (Drafting suggestions): ‘4. Paragraphs 1, 2 and 3 shall not apply where **and insofar as the data subject has the information and where** the personal data ~~have been~~**are** collected in the context of a ~~clear and~~**direct, limited and clearly** circumscribed relationship between data subjects and a controller exercising an activity that is not ~~data-intensive~~**likely to result in a high risk to the rights and freedoms of data subjects nor involve ~~the~~ large scale processing ~~of large amounts~~ of personal data, special categories of personal data or complex processing operations** and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1~~, unless~~**.** **The first subparagraph shall not apply where** the controller **intends to process the data collected from the data subject for other purposes,** transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.’ AT (Comments): • AT can support the compromise proposal on Article 13(4) and Recital 36 GDPR. The proposed amendments provide important clarifications. • For further clarification, “large scale processing of personal data” could be used (instead of „processing of large amounts of personal data“). That term is also used in other GDPR provisions and covered in EDPB guidelines. ES (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
	13.4. Paragraphs 1, 2 and 3 shall not apply where personal data have been collected in the context of a clear and Delimited relationship between the data subjects and a controller carrying out an activity that does not require intensive use of data, and there are reasonable grounds to assume that the data subject has already the information referred to in points (a) and (c) of paragraph 1, ***unless the controller is a public authority or public body or a private entity for the performance of a task in the public interest****, transmits the data to other recipients or categories of recipients, transfers them to a third country, carries out automated decision-making, including profiling, as referred to in Article 35 (1), or the processing is likely to entail a high risk to the rights and freedoms of data subjects within the meaning of Article 35.* ES (Comments): Precise new regulation can be beneficial in terms of simplification and burden reduction for some stakeholders, but without regulatory quality it can lead to even greater uncertainty. That is why the new exemption from the duty to report in 'clear and circumscribed relationships' and 'non-data-intensive' activities is ambiguous and creates legal uncertainty, especially for SMEs. See recital (36). The problem may lie more in 'when' and 'how' it is reported, rather than in the duty itself. For example, it might be useful to allow information to be provided in layers or at more flexible times, but to maintain the rights of the data subject. It may be necessary to analyse whether this is a real problem for SMEs. Consideration should also be given to the asymmetry that can be created by different regulation between the public and private sectors, starting with a stricter duty of information for the public sector.

Presidency compromise text	Drafting suggestions and Comments
	The aims of the position are to • Support COM objective • Clarify terminological ambiguity: the concept of 'not data-intensive' as well as the concepts of 'clear and circumscribed relationship' or 'reasonable grounds'. • Consider the model of providing information in layers. • Standardise public/private sector We therefore propose the following alternative wording (and the corresponding alternative wording proposed for recital 36):
6. In Article 13, paragraph 5 is added:	
'5. When the **further** processing takes place for scientific research purposes **by the same controller and where and insofar as**~~and~~ the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort ~~subject to the conditions and safeguards referred to in Article 89(1)~~ or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that **further** processing**, subject to the conditions and safeguards referred to in Article 89(1)**, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take	AT (Comments): Provided that the definition for „scientific research" is deleted, AT can support the compromise proposal ES (Comments): We support the COM proposal which seeks to provide legal certainty for researchers by validating the "legitimate interest" as a clear legal avenue, but recalling that there

Presidency compromise text	Drafting suggestions and Comments
appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.'	is still a need to balance this interest with the rights and freedoms of natural persons. We support the wording of the COM with the amendments already included. LV (Comments): LV supports the Presidency's proposed compromise text.
~~7. In Article 22, paragraphs 1 and 2 are replaced by the following:~~	AT (Comments): AT can support deleting the amendment of Article 22 ES (Drafting suggestions): *'1. A decision which produces legal effects concerning a data subject or similarly significantly affects him or her may be based solely or substantially on automated processing, including profiling.* *2. In the cases referred to in paragraph 1, the controller shall ensure at least the right of the data subject to obtain human intervention, to express his or her point of view, to challenge the decision and the right to explicability of the automated decision, which shall include access to clear, comprehensible and meaningful information on the criteria, determining factors and merits of the decision as well as on its consequences for the data subject.* *3. Where the decisions referred to in paragraph 1 are taken through the use of artificial intelligence systems, the controller shall take into account the nature and*

Presidency compromise text	Drafting suggestions and Comments
	level of risk of the system for the purposes of implementing the safeguards provided for in this Article.' ES (Comments): • **Article 22 on automated decision-making** We welcome the amendment to Article 22 GDPR, as the starting point of a blanket ban seems obsolete and it is through a 'right' whose legal existence has been questioned by the same EDPB. The new paradigm in which only automated decisions are considered to be a particularly risky context requiring particular safeguards is welcome. Facilitating their use in the execution of contracts is welcome. It is also positive that the recital directly introduces the principle of necessity with specific reference to the absence of other "equally effective" means. Some discretion should be given to the controller to make this assessment. On the negative side, this opportunity to reform Article 22 should be seized. Among other improvements, one could follow the line and introduce the application of these safeguards with regard to 'substantially' automated decision-making in line with Article 6 (3) RIA and the case-law of the CJEU, i.e. not only to 'solely automated' decisions. The improvements on transparency and explainability of the CJEU 2023 and 2025 should be introduced. It should be assessed whether to make specific reference to the higher intensity of safeguards for the use of technologies such as artificial intelligence, especially in AIR high-risk scenarios.

Presidency compromise text	Drafting suggestions and Comments
	It would also be desirable to explicitly regulate the right to explainability and for data protection to be its special legal basis, to which Article 86 AI Act refers. With regard to the right to *ex-post human oversight,* some clarification should be included along the lines of certain documents such as those produced by the Dutch data protection authority or the EDPS. Clarify the status of subjective rights in Article 22 GDPR and its connection with the limits of Article 23 GDPR. The objectives we are looking for in our position are: • Ensure the effective application of the safeguards of Article 22 when the decision is based or substantially determined by an automated system, even if there is also some human intervention. • Recognise the rights of the data subject in these contexts and in particular the right to explainability of automated decision, ensuring access to understandable information about its criteria, rationale and consequences. • Ensure a proportionate and contextualised application of the safeguards of Article 22 when decisions are taken by means of artificial intelligence systems, taking into account the nature and level of risk of the system We therefore propose the following wording: LV (Comments): LV considers it important to retain the amendments concerning Article 22 and to continue discussions on their clarification. This is essential for ensuring the

Presidency compromise text	Drafting suggestions and Comments
	systemic coherence of the GDPR, legal certainty, and its practical application across Member States. SE (Comments): Sweden would like to ask if it would be possible to further elaborate the reasons for the deletion of the Commission's proposal in this regard.
~~'1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:~~	
~~(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;~~	
~~(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or~~	
~~(c) is based on the data subject's explicit consent.'~~	
8. Article 33 is amended as follows:	

Presidency compromise text	Drafting suggestions and Comments
(a) paragraph 1 is replaced by the following:	
'1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~96~~**72** hours after having become aware of it, notify the personal data breach **[**via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555**]** to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.'	AT (Drafting suggestions): '1. In the case of a personal data breach that is likely to result in ~~**a high risk**~~ **an "impactful risk" ["relevant risk"/"increased risk"]** to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~96~~**72** hours after having become aware of it, notify the personal data breach **[**via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555**]** to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within ~~**96**~~**72** hours, it shall be accompanied by reasons for the delay.' AT (Comments): • AT remains sceptical about raising the threshold for data breach notifications to the supervisory authority. • A possible compromise could be to use a threshold between "risk" and "high risk", such as "impactful risk", "relevant risk", "increased risk" or likewise • AT generally supports the alignment of time-limits in different legal acts • AT supports maintaining the 72 hours time-limit (which also has to be aligned in the last sentence) ES (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
	'1. In the case of a personal data breach the controller shall without undue delay and, where feasible, not later than 48 hours after having become aware of it, notify the personal data breach via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56. Where the notification to the supervisory authority is not made within 48 hours, it shall be measured by reasons for the delay.' LV (Comments): LV supports the Presidency's proposed compromise text. SE (Drafting suggestions): In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~96~~**72** hours after having become aware of it, notify the personal data breach **[**~~via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555~~**]** to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.' SE (Comments): Sweden is in favour of keeping the initial time limit of 96 hours as proposed by the Commission. Sweden is also in favour of incidents being reported to national authorities, not via SEP.

Presidency compromise text	Drafting suggestions and Comments
(b) the following paragraph is added:	ES (Comments): • **Article 33 (2) on the single entry point**: we can agree with the French proposal
'1a. Until the establishment of the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56 **of this Regulation**.'	LV (Comments): LV supports the Presidency's proposed compromise text. SE (Comments): See comment above regarding Sweden's position on SEP.
(c) the following paragraphs are added:	
'6. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person **and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists**~~. The proposals~~ shall be ~~submitted to the Commission~~**available** within [OP date = nine months of the entry into application of this Regulation]. ~~The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an~~	AT (Comments): • AT supports that the common template for data breach notifications and the lists of circumstances relating to the risk threshold are established by the EDPB. • For structural reasons, all respective provisions should be moved to Article 70 GDPR, where all tasks of the EDPB are regulated. SE (Comments):

Presidency compromise text	Drafting suggestions and Comments
~~implementing act in accordance with the examination procedure set out in Article 93(2).~~	Sweden is in favour of allowing for the Commission to adopt implementing acts in accordance with comitology procedure set out in Article 93(2) of the GDPR. However, Sweden is in favour of the Presidency proposal with regards to the preparation of a list of non-high risk circumstances.
7. The template and ~~the list~~**lists** referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. ~~The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6.'~~	AT (Comments): Move to Article 70 (see comment on Article 33(6))
9. Article 35 is amended as follows:	ES (Drafting suggestions): *Article 35 is amended as follows:* (a) modify the following paragraph: *10. Where processing pursuant to point (c) or (e) of Article 6 (1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment should be carried out as part of a general impact assessment in the context of the adoption of that legal basis, that be specific in the minimum instances and measures to be monitored by controllers that are subject, the law paragraphs 1 to 7 shall not apply unless Member States deem it necessary to carry out such an assessment prior to processing activities.*

Presidency compromise text	Drafting suggestions and Comments
	(b) the following paragraphs are inserted: *6th. The Board shall prepare a template for documenting the process of the data protection impact assessment and a methodology for conducting data protection impact assessments. Both, template and methodology, should lay down minimum requirements applicable to process that means a DPIA and its documentation, and regarding with the principle of accountability, should be adjusted for each processing activity taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and frequencies of natural persons. They will be reviewed at least every three years and updated where necessary.* *The template and methodology shall be submitted to the Commission within [OP date = 9 months of the entry into application of this Regulation]. The Commission is considering to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93 (2).* ES (Comments): With regard to Article 35, there are concerns that carrying out the Data Protection Impact Assessment (DPIA) is one of the most important safeguards for enabling processing, even in the same Omnibus proposal. The DPIA is an ongoing and dynamic procedure and the message that it is the Commission that has the final say in the decision to reduce it to a template that can turn it into a mere formalistic *checklist* would weaken the risk-based approach and effective safeguards for rights and freedoms. Furthermore, the proposal to apply a

Presidency compromise text	Drafting suggestions and Comments
	single methodology may negatively affect the development of innovative DPIA solutions, particularly in changing technological environments. We therefore propose the following wording:
(a) paragraphs 4, 5 and 6 are replaced by the following:	
'4. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.	AT (Comments): • AT supports harmonisation with regard to the data protection impact assessment and welcomes that the respective competences are assigned to the EDPB. • For structural reasons, all respective provisions should be moved to Article 70 GDPR, where all tasks of the EDPB are regulated SE (Comments): Sweden is in favour of allowing for the Commission to adopt implementing acts in accordance with comitology procedure set out in Article 93(2) of the GDPR.
5. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** a list of the kind of processing operations for which no data protection impact assessment is required.	AT (Comments): Move to Article 70 (see comment on Article 35(4))

Presidency compromise text	Drafting suggestions and Comments
6. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** a common template and a common methodology for conducting data protection impact assessments.'	AT (Comments): Move to Article 70 (see comment on Article 35(4))
(b) the following ~~paragraphs are~~**paragraph is** inserted:	
~~'6a. The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission within [OP date = 9 months of the entry into application of this Regulation]. The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).~~	SE (Comments): See comments above.
~~6b. The lists and the template and methodology referred to in paragraph 6a shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a.~~	
6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the ~~Commission adopts the implementing act~~**Board establishes and makes public the lists** referred to in paragraph ~~6a~~**4 and 5**.'	AT (Comments): Move to Article 70 (see comment on Article 35(4))

Presidency compromise text	Drafting suggestions and Comments
10. ~~The following article is added:~~	
~~'Article 41a~~	
~~(1) The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.~~	AT (Comments): AT supports assigning the competence to issue guidelines regarding pseudonymisation and identifiability of a natural person to the EDPB.
~~(2) For the purpose of paragraph 1 the Commission shall:~~	
~~(a) assess the state of the art of available techniques;~~	
~~(b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.~~	
~~(3) The implementation of the means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.~~	
~~(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.~~	

Presidency compromise text	Drafting suggestions and Comments
~~(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).'~~	
11. In Article 57(1) is amended as follows:	
(a) point (k) is deleted;	
	AT (Drafting suggestions): **11a. Article 57(4) is amended as follows:** **'4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character <u>or where an abusive intention on the part of the data subject submitting those requests can be demonstrated</u>, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request<u>, or that the request is submitted with an abusive intention</u>.'** AT (Comments): • In order to maintain consistency, Art. 57(4) should be amended in line with Art. 12(5) (see also § 59 of the EDPB/EDPS opinion) • See proposal for corresponding Recital 35a
12. In Article 64(1), point (a) is deleted.	

Presidency compromise text	Drafting suggestions and Comments
13. In Article 70(1), point (h) is deleted.	
14. In Article 70(1), the following points are inserted:	
'(ha) ~~prepare and transmit to the Commission a proposal for~~**establish** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35.	SE (Comments): See comments above.
(hb) ~~prepare and transmit to the Commission a proposal for~~**establish** a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35.	
(hc) ~~prepare and transmit to the Commission a proposal for~~**establish** a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person pursuant to Article 33 **and a list of the circumstances in which it is not likely to result in such a high risk**	AT (Drafting suggestions): (hc) ~~prepare and transmit to the Commission a proposal for~~**establish** a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in ~~**a high risk**~~ **an "impactful risk" ["relevant risk"/"increased risk"]** to the rights and freedoms of a natural person pursuant to Article 33 **and a list of the circumstances in which it is not likely to result in such ~~a high risk~~ an "impactful risk" ["relevant risk"/"increased risk"]** AT (Comments): See comments on Article 33(1)

Presidency compromise text	Drafting suggestions and Comments
hca issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph on pseudonymisation, clarifying circumstances whether a natural person is identifiable and means reasonably likely to be used to identify a natural person, and specifying means and criteria to determine whether data resulting from pseudonymisation may no longer constitute personal data for certain entities'	AT (Comments): AT can support the compromise proposal
15. After Article 88, the following articles are added:	
'Article 88a	AT (Comments): See previous AT comments/proposals SE (Comments): Sweden considers that the proposed introduction of the provisions governing cookies and machine-readable consent in one legal protection framework is considered prone to realise the objectives of clarifying and simplifying the digital legal framework. The practical implications of the proposed provisions and the introduction into the GDPR are still subject to examination, e.g. with regards to the interplay between the e-privacy directive and the GDPR.
Processing of personal data in the terminal equipment of natural persons	

Presidency compromise text	Drafting suggestions and Comments
(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.	LV (Comments): Article 5(3) of the ePrivacy Directive acts as lex specialis in the field of electronic communications, ensuring the integrity of the user's terminal equipment and protecting it against any unauthorised access to, or retrieval of, information stored therein, irrespective of whether such information qualifies as personal data. This provision applies to a broad range of technologies, including cookies and other similar technologies that enable access to, or the use of, information stored in the user's terminal equipment. Accordingly, the ePrivacy Directive framework protects not only the processing of personal data, but also the privacy of terminal equipment, the confidentiality of communications, and the user's control over their device as such. In light of the above, the simple transfer of the ePrivacy Directive's regulatory approach into the GDPR, without a thorough assessment of its compatibility with the GDPR's system and structure, could unduly expand the scope of the Regulation, affect the coherence of the current regulatory framework, and create additional uncertainty regarding the delineation between the ePrivacy and GDPR regimes. LV therefore calls on Member States to continue discussions on the potential impact of transferring the ePrivacy Directive's provisions into the GDPR and on the implications for the scope of the GDPR. In addition, Article 88a(1) should be complemented to explicitly cover ''subsequent processing'' as well.
(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).	

Presidency compromise text	Drafting suggestions and Comments
(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:	LV (Drafting suggestions): (3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful, **subject to the conditions of Article 6**, to the extent it is necessary for any of the following: LV (Comments): LV emphasises that Article 88a(3) should be explicitly linked to Article 6 of the GDPR in order to ensure consistency with the Regulation's systemic structure, under which Article 6 exhaustively defines the conditions for the lawfulness of processing. In the absence of such a link, point 3 would de facto introduce additional conditions for the lawfulness of processing that are not set out in Article 6 of the GDPR and would create inconsistencies with its internal coherence and rationale.
(a) carrying out the transmission of an electronic communication over an electronic communications network;	
(b) providing a service explicitly requested by the data subject;	
(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;	SE (Comments):

Presidency compromise text	Drafting suggestions and Comments
	Sweden is in favour of the objectives pursued by the proposed exemptions set out in Article 88a(3)(c) and Article 88a(3)(d) and considers that the proposed provisions are prone to strike a fair balance between the interests of controllers on the one hand and the protection of privacy of the data subjects on the other. Controllers must be able to rely on third parties providing for audience measurement services. This should be reflected in the said provision, e.g. by specifying that the service can be carried out on behalf of the controller.
(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.	LV (Comments): LV has previously emphasised that the ePrivacy Directive primarily protects the privacy and integrity of the user's terminal equipment, rather than only the processing of personal data stored therein. Accordingly, access to terminal equipment without the user's consent, where such access is justified by broader security considerations, may significantly affect access- control mechanisms and undermine the user's effective ability to determine who accesses their device, to what extent and at what point in time. At the same time, the proposed exception permitting access to terminal equipment for the purposes of "maintaining" or "restoring" security relies on concepts which, by their nature, are technically flexible and open to interpretation. This creates a risk that service providers may interpret these notions broadly, rely on them to justify various forms of data retrieval from the device, and thereby effectively expand the scope of access beyond the original objectives of the regulatory framework. LV therefore proposes the deletion of Article 88a(3)(d).

Presidency compromise text	Drafting suggestions and Comments
(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:	
(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;	
(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;	
(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.	
This paragraph also applies to the subsequent processing of personal data based on consent.	
(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]	
Article 88b	AT (Comments): See previous AT comments/proposals

Presidency compromise text	Drafting suggestions and Comments
Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons	SE (Comments): Even though Sweden is in favour of the objectives pursued by the proposed provision, we are concerned about the practical implications thereof, e.g. with regards to the risk of market concentration to a few platform operators which could result in distortion of competition, as well as the consequences for certain actors, such as media service providers. Considering these implications, Sweden is in favour of pursuing discussions in this regard.
(1) Controllers shall ensure that their online interfaces allow data subjects to:	
(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;	
(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.	
(2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1.	
(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.	LV (Comments):

Presidency compromise text	Drafting suggestions and Comments
	LV proposes to delete Article 88b(3), as the envisaged exemption for media service providers poses risks to data subjects' rights. By allowing media service providers to disregard machine- readable preference signals, the exemption would undermine users' ability to rely on a consistent and predictable level of protection, create regulatory fragmentation, and weaken the effective implementation of the framework, since the exercise of rights would become dependent on the provider's sectoral status. While media freedom is a fundamental element of democracy, sector- specific exemptions must not lower the level of data protection or diminish the predictability and coherence of users' rights. If Member States decide to retain this point, it should be clarified that the exemption also extends to processors and independent audience measurement providers acting on behalf of media service providers. Without such clarification, third- party scripts essential for audience measurement could be blocked at browser level before the user accesses the media service, thereby rendering the exemption ineffective in practice.
(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices.	
Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.	

Presidency compromise text	Drafting suggestions and Comments
(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].	
(6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.	
(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].	
Article 88c	AT (Comments): See previous AT comments/proposals ES (Drafting suggestions): We therefore propose the following wording: *Article 88c. Legitimate interest and treatments for artificial intelligence systems and models* *The processing of personal data carried out for the lifecycle of an artificial intelligence system or model, where functionally necessary for its lawful design, development or use, may be based on the legitimate interest of the controller or of a third party for the purposes of Article 6(1)(f). Among the various elements of the weighting, account*

Presidency compromise text	Drafting suggestions and Comments
	shall be taken of the fact that the controller identifies and implements governance, security and control measures proportionate to the risks of the processing. For this purpose, it shall be sufficient to demonstrate that, in the current state of the art, the use of anonymised or synthetic data does not offer equivalent functionality, quality or reliability for the purpose pursued. It shall also assess the nature and volume of the data processed, the reasonable predictability of the processing for the data subjects, taking into account the source and the context of obtaining the data, as well as the existence of appropriate technical and organisational measures. *Where, due to the nature or complexity of the system or model, the data subject's right to object cannot produce immediate individual effects, the controller shall take and document equivalent, structural and verifiable measures aimed at reasonably mitigating the impact of the processing.* *The provisions of this Article shall also apply to public sector authorities and bodies, even when acting in the exercise of their functions, where the exclusion provided for in Article 6(1)(f) does not apply subject to the safeguards set out in this Article.* ES (Comments): The position aims to: • Expressly and legally secure recognition that legitimate interest can serve as a basis for processing personal data throughout the lifecycle of AI systems and models, avoiding interpretative uncertainties and ex ante blockages resulting from a strict application of schemes designed for traditional processing. • Circumscribe such use of legitimate interest by functional and weighting criteria linked to the design and operation of the system, without resorting to closed lists

Presidency compromise text	Drafting suggestions and Comments
	of purposes or rigid technical requirements that would limit innovation or quickly become obsolete. • Align the application of the GDPR with the technical reality of advanced AI systems, in particular those of high complexity or generative nature, where classical mechanisms of immediate individual control are not always feasible or verifiable. • Ensure effective protection of rights, such as opposition when it becomes an obligation to comply, by redirecting the exercise of rights such as opposition towards structural, verifiable and proportionate solutions to the actual impact of the processing. • Allow public sector authorities and bodies to also rely on legitimate interest for the processing of personal data linked to the development and use of artificial intelligence systems, including when acting in the exercise of their tasks, without requiring a specific legal empowerment, subject to the requirements and safeguards provided for in the provision. LV (Comments): LV proposes to delete Article 88c, since the proposed Article 88c, by its substance and regulatory purpose, should be included in the AI Act rather than in the GDPR. The GDPR has so far been designed as a technologically neutral legal act, establishing general rules for the processing of personal data irrespective of the technologies used. Introducing regulation that is tailored to specific technologies into the GDPR could undermine the systemic coherence of the Regulation and weaken its technological neutrality, as well as create risks of normative overlap with the sector- specific provisions laid down in the AI Act.

Presidency compromise text	Drafting suggestions and Comments
Processing in the context of the development and operation of AI	
Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	SE (Comments): Sweden is in favour of the ambition to bring greater legal certainty to the development and operation of AI systems and removing disproportionate obstacles to such development and use. Nevertheless, as Article 6(1)(f) does not apply to authorities when performing their tasks, it is important that the proposed clarification in Article 88c is not interpreted in a way which may alter or affect the possibilities available to the public sector to process data for the said purposes.
Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'	
Article 10 **Repeals and transitory clauses**	
– 1. Regulation 2019/1150/EU is repealed with effect from [date = entry into application of this Regulation].	AT (Drafting suggestions):

Presidency compromise text	Drafting suggestions and Comments
	1. Regulation 2019/1150/EU is **partially** repealed with effect from [date = entry into application of this Regulation].
– 2. By way of derogation from paragraph 1, the following provisions shall continue to apply until 31 December 2032:	AT (Drafting suggestions): 2. **In accordance with** ~~By way of derogation from~~ paragraph 1, the following provisions shall continue to apply ~~until 31 December 2032~~: AT (Comments): AT comments: Firstly, we would like to refer to our common position with BE, NL and IT: A differentiated approach is needed rather than the outright repeal of all provisions of the P2B Regulation, in the interest of protecting SMEs. In general, we welcome simplifications as we see certain overlaps between the P2B Regulation and the Digital Services Act (DSA) and the Digital Markets Act (DMA). We are open to discuss the repeal of individual provisions that overlap—especially transparency obligations—as there is leeway to interpret some of them in existing DSA obligations (esp. Art. 14, or also Art. 27 DSA). The Commission could clarify those by means of guidelines. However, the P2B Regulation addresses specific business issues in the relationship between businesses and platforms. From our point of view, the obligations of the P2B Regulation can be divided into two types: transparency and material obligations. The latter are particularly important to us, as there is no appropriate equivalent in other legal acts such as the Digital Services Act (DSA). In general, the most important provisions for us are: Articles 3 (in particular para. 2), 4 and 11.

Presidency compromise text	Drafting suggestions and Comments
	Further important provisions are found in Articles 5, 7, 10 and 15. They all require legal certainty beyond 2032. Therefore, we propose to maintain those Articles on a permanent basis. An alternative could be foreseeing an evaluation by 2032 as a review has not yet taken place; we do not have an impact assessment. On the contrary, the document on the interaction of the DSA with other legal acts (COM (2025) 368 final), highlights the added value of the P2B Regulation. We therefore need a full review to determine whether the two legal acts (DMA and DSA) are sufficient and, if necessary, which provisions need to be transferred (e.g. into the DSA) to protect business users—including SMEs—before repealing the P2B Regulation.
	AT (Drafting suggestions): **(-a) Article 1;** AT (Comments): Article 1 must be maintained because it sets out the scope and subject matter of the P2B Regulation, which are necessary elements for the proper application of the other provisions that remain in force.
(a) Article 2, point (1);	AT (Drafting suggestions): Article 2, point**s** ~~(5);~~ **(1) to (10) and (13);** AT (Comments): These definitions are needed for the provisions which should not to be repealed.

Presidency compromise text	Drafting suggestions and Comments
(b) Article 2, point (2);	AT (Drafting suggestions): ~~(b) Article 2, point (2);~~
(c) Article 2, point (5);	AT (Drafting suggestions): ~~(c) Article 2, point (5);~~
	AT (Drafting suggestions): **(ca) Article 3;** AT (Comments): Article 3 contains important material and transparency obligations. First, without the material obligation in Article 3.2, business users will no longer be informed before terms and conditions are changed and they will lose the right to terminate the agreement on these grounds. This harms the business user's position in their relation to the platform by weakening contractual transparency and predictability In addition to the material obligation of Article 3(2) mentioned above, the transparency obligations set out in Article 3 offer considerable protection to business users, particularly since non-compliant terms and conditions are automatically null and void. The repeal of Article 3 would remove an important safeguard for business users against arbitrary enforcement, thereby depriving them of the right to be informed in advance, in a clear and comprehensible manner, of the potential conditions under which the service may be restricted, irrespective of the size of the platform.
(d) Article 4;	AT

Presidency compromise text	Drafting suggestions and Comments
	(Comments): Article 4.2 is particularly important to AT. Its repeal in 2032 would lead to business users no longer being granted a notice period before their access to the platform services is terminated. This prevents them from taking appropriate measures or challenging the termination decision before it takes effect, rendering them vulnerable to arbitrary decisions by the platform.
	AT (Drafting suggestions): **(da) Article 5;** **(db) Article 7;** **(dc) Article 10 ;** AT (Comments): The key transparency obligations in Articles 5 and 7 should be maintained. Repealing Article 5 would shift the enforcement of these issues away from national regulators and risk reducing the accessibility and effectiveness of redress for SMEs operating on platforms. Without Article 7, in turn, platforms are free to put business users at a disadvantage where they compete with the platform's own products and services, or with other business users controlled by the platform, without disclosure. Because there is no obligation of any kind to be transparent, business users will not be able to know whether, how and why this is happening. The transparency required by Article 7 provides insight into the different forms of differentiated treatment and enables authorities, including those under the DMA and competition law, to detect and address such practices. Article 10 is important to business users and should also be maintained. As most platforms are not gatekeepers, its repeal will allow them to impose

Presidency compromise text	Drafting suggestions and Comments
	parity clauses without transparency. They will not need to provide any justification and prospective business users will not know such restrictions exist. This lack of transparency will make it significantly more difficult for authorities to gain insight into these practices and for affected business users to challenge them. For the sake of completeness, we would also like to point out that the prohibition of retroactive changes to terms and conditions (Art 8 (a)) is a material obligation which has added value for business users, esp. SMEs.
(e) Article 11;	AT (Comments): Dedicated complaint channels for business users are important. The repeal of Article 11 in 2032 severely limits the business user's ability to challenge unfair or illegal conduct through an internal complaint-handling system. While they will still have access to an internal complaint handling system under the DSA, its scope is limited to illegal content or alleged violations of the platform's terms and conditions and in time. This in turn leaves the business user without quick and effective remedies against P2B non-compliance by the platform, technological issues or any other measures taken by the platform in the context of providing intermediation services that affect the business user.
(f) Article 15.	AT (Comments): In order to ensure the flexibility for Member States, the enforcement system should not be changed and be open to the Member States. (E.g. enforcement in AT should continue to be carried out by means of legal action brought by representative organisations or associations and by public bodies in accordance with Article 14; if necessary, this should therefore also be retained.)

Presidency compromise text	Drafting suggestions and Comments
	AT (Drafting suggestions): **(fa) Article 19** AT (Comments): Article 19 must remain in force to maintain coherence of the Regulation following its partial repeal. We believe its removal will lead to ambiguity and legal uncertainty. ES (Drafting suggestions): ***Article 49 Derogations for specific situations*** ***Option 1*** *(…)* *4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.* *This shall include cases where the transfer is necessary for the implementation, application or compliance with international or administrative agreements on mutual assistance or cooperation concluded by a Member State, including cases where personal data is exchange on a large scale and in a systematic manner, and where such agreements do not provide for appropriate safeguards within the meaning of Article 46. In such cases, Member States shall ensure that appropriate safeguards for the protection of data subjects are provided for under Union law or the law of the Member State, including personal data in transit as well as after such transaction has taken place.*

Presidency compromise text	Drafting suggestions and Comments
	Personal data shall not be transferred where the competent authority responsible for the transfer considers that the rights and freedoms of the data subject concerned override the public interest pursued by the transfer. *Transfers based on this Article shall be documented.* ***Option 2*** *1. (...)* *Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.* *The requirement that the transfer be non-repetitive shall not apply to transfers based on point (d) of the first subparagraph, where such transfers are necessary for important reasons of public interest recognised in Union law or in the law of a Member State, including transfers carried out pursuant to international or administrative agreements on mutual assistance or cooperation.* ES

Presidency compromise text	Drafting suggestions and Comments
	(Comments): The purpose of this amendment is to clarify and specify the scope of the derogation for important reasons of public interest laid down in Article 49 of Regulation (EU) 2016/679, in particular as regards international data transfers carried out in the context of periodic exchanges of information between public authorities. The proposed amendment clarifies that the important public interest referred to in Article 49(1)(d) explicitly encompasses situations in which a transfer of personal data is necessary for the implementation, application or compliance with international or administrative agreements on mutual assistance or cooperation concluded by a Member State. It further specifies that, where such agreements do not themselves provide for appropriate safeguards for the protection of personal data, Member States must ensure that such safeguards are provided for under Union law or the law of the Member State concerned. In addition, the amendment clarifies that transfers necessary for important reasons of public interest under Article 49(1)(d), including those carried out pursuant to international or administrative cooperation agreements, may in practice take place on a recurring basis. It therefore specifies that the requirement of non-repetitiveness, which applies to the residual ground of compelling legitimate interests, should not be understood as limiting such public interest transfers. This clarification does not affect the exceptional nature of Article 49 derogations, which remain subject to strict necessity, proportionality and appropriate safeguards ensuring a high level of protection of personal data. In this respect, the approach reflected in the amendment is consistent with solutions already recognised in Union law, notably in Article 37(1) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. That provision allows transfers of personal data for important public interest purposes, such as the prevention and combating of crime, in the absence of an adequacy decision, where appropriate safeguards are provided either in a legally binding instrument or based on a documented assessment of all the circumstances surrounding the transfer. Without affecting the distinct scope and objectives of the GDPR, the present amendment similarly clarifies that transfers based on important reasons of public interest may rely on safeguards embedded in the relevant agreement or, where such

Presidency compromise text	Drafting suggestions and Comments
	safeguards are absent, on appropriate safeguards laid down in Union or national law, following a prior and documented assessment by the competent authority as part of the data protection impact assessment, carried out, for example, in the context of the negotiation of the agreement.

Consultation GDPR/P2B/E-Privacy Deadline: ***18 March 2026***
From: BE, CZ, DK, FI, IE, IT, LU, NL, SI **Updated: 19/03/2026 15:56**

Guidelines to be followed

Please kindly provide your contributions in the table below.

Drafting suggestions: you may use '**track changes**'* or formatting (for example **bold-underline** for additions and ~~strike-through~~ for deletions, **where necessary, in a different colour**). *Track changes can only be connected once the cursor is placed in editable areas (Drafting or Comments columns).

To make it feasible to consolidate all contributions, the structure of the table must not be changed, so **no rows can be added or deleted.**

New provisions may only be added in any of the **'existing cells'.**

Name of document: please add the **two initials** of your delegation's country followed by a space (to the MS Word document name), followed by any optional text, for example, for Austria: **AT comments on … .docx**

Thank you for your cooperation!

Presidency first compromise text	Drafting suggestions and Comments
General Comments	FI (Comments): Finland thanks the Presidency and the Commission for the preparations. Finland is still in progress of forming our formal position. Below are our preliminary comments. We thus reserve the possibility to further specify our comments and suggestions in due course. LU (Comments): A. CY Presidency discussion note **Question 1:** delegations are invited to express their views on the proposed provisio a) the processing of personal data in the context of the development and systems based on the lawful ground of legitimate interest (Art 88c).

Presidency first compromise text	Drafting suggestions and Comments
	b) the proposed new derogation from the prohibition on processing special cat personal data (Article 9 (2)(k) and (5). **Reply:** Both these proposals are still under examination at national level. **Question 2**: delegations are invited to express their views and possible suggestions c exemptions from consent requirement for aggregated information for measuring the a maintaining or restoring the security of a service or the terminal equipment. In Presidency invites delegations to share their positions on the two following points: Should the exemption for audience measurement remain limited to its originally inte the controller of a service requested by a data subject) or more open, in particular c actors it should cover (other parties in the measurement value chain that are not p controller)? Should the exemption for safeguarding the security of a service or a device be furth delineated? **Reply:** Luxembourg is currently performing an analysis of the conditions under which data used for audience measurement and security purposes are exempted from consent. We consider it important to clarify, among others, the two following points: o Concerning audience measurement, we identify, at this stage, a need to clarify the notion of "subsequent processing", in comparison to that of "further processing" in articles 5 and 6 of the GDPR.

Presidency first compromise text	Drafting suggestions and Comments
	○ With regards to security purposes, which is the **threshold at which a security-related purpose would justify the application of such an exemption?** The answer to this question is important to further assess the compatibility of this provision with the principle of proportionality. **Question 3:** Delegations are invited to share their views and overall position on tl Article 88b GDPR on automated and machine-readable indications of data subje respect to processing of personal data in the terminal equipment of natural person **Reply:** The analysis of this provision is ongoing. As a general remark, Luxembourg would like to support this measure in so reduce "Cookie fatigue", that impacts every internet user and influences l engage with digital services daily. It moreover globally supports paragraph 3 of proposed article 88b, that exception in favor of media service providers.

Presidency first compromise text	Drafting suggestions and Comments
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2022/2554, and (EU) 910/2014 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)	BE (Drafting suggestions): **REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2022/2554, and (EU) 910/2014 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, partially repealing Regulation (EU) 2019/1150 and repealing Regulations (EU) 2018/1807, ~~(EU) 2019/1150,~~ (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)** BE (Comments): As set out in our comments on recital 59 and article 10, Belgium proposes repealing only part of the P2B Regulation. IT (Drafting suggestions): **REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2022/2554, and (EU) 910/2014 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, partially repealing Regulation (EU) 2019/1150 and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)** IT (Comments): As set out in our comments on recital 59 and article 10, ITALY proposes repealing only part of the P2B Regulation.

Presidency first compromise text	Drafting suggestions and Comments
	SI (Comments): In general, we support the direction taken by the Presidency's compromise text; however, we will submit more specific proposals for rewording, if necessary, once the full compromise text, which will include Articles 88a-88c, is available.
(27) ~~This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an identified or identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data, it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for those third parties who have such means at their disposal. An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. In this respect the Court~~	BE (Comments): Belgium supports the deletion of the proposed amendment to Art. 4 (1). The proposed amendment risked creating significant legal uncertainty across the data ecosystem and undermining compliance with other EU digital legislation that cross-references the GDPR definition. DK (Comments): DK considers it important to define the concept of relative anonymisation in order to ensure a greater degree of uniformity in enforcement. Furthermore, DK notes the importance of this definition aligning with CJEU case law as pertaining to the C-413/23 P EDPS v SRB case. FI (Comments): Finland supports deleting recital 27. As the changes to the definition for personal data are deleted, Finland considers that the accompanying recitals should accordingly be deleted.

Presidency first compromise text	Drafting suggestions and Comments
~~of Justice of the European Union has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council[1]. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria in an implementing act.~~ 1 ~~Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj)~~	
(27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable. The European Data Protection Board should support controllers by adopting guidelines assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to pseudonymise personal data effectively, and clarifying circumstances whether a natural person is identifiable and means reasonably likely to be used to identify a natural person, including means and criteria to determine whether data resulting from pseudonymisation may no longer constitute personal data for certain entities. While controllers remain fully responsible to	BE (Comments): Belgium welcomes the approach of empowering the EDPB to issue guidelines on pseudonymisation criteria and to ensure legal certainty we encourage the EDPB to prioritise publication of these guidelines promptly after entry into force. CZ (Drafting suggestions): **(27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union, it is important to**

Presidency first compromise text	Drafting suggestions and Comments
determine whether data resulting from pseudonymisation is personal, the guidelines should support controllers in implementing such measures and criteria, and provide guidance to demonstrate whether pseudonymised data do not lead to re-identification of data subjects.	**provide further clarity on when a natural person should be considered to be identifiable. The Commission, together with the European Data Protection Board, should support controllers by adopting an implementing act assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to pseudonymise personal data effectively, and clarifying circumstances whether a natural person is identifiable and means reasonably likely to be used to identify a natural person, including means and criteria to determine whether data resulting from pseudonymisation may no longer constitute personal data for certain entities. ~~While controllers remain fully responsible to determine whether data resulting from pseudonymisation is personal, the guidelines should support controllers in implementing such measures and criteria, and provide guidance to demonstrate whether pseudonymised data do not lead to re-identification of data subjects.~~** CZ (Comments): CZ: CZ believes that an implementing act is much more preferable in terms of legal certainty and uniform application within EU, with at least the standard benefits for demonstrating compliance that are used Art. 24, 25, 28, 32 GDPR. It is a substantial factor of Digital Omnibus having an economic impact. CZ believes that at least Article 41a must be retained to preserve added value of Digital Omnibus to European economy. FI (Drafting suggestions): Delete recital 27a. FI

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): As the changes to the definition for personal data are deleted, Finland considers that the accompanying recitals should accordingly be deleted. LU (Comments): • **The definition of "personal data"** - Article 4 (a) in the CP read together with preamble (27a) The definition of personal data in the GDPR should remain unchanged. The CJEU's case law, that is legally binding, ensures that the notion of "personal data" remains both legally robust and adaptable. Introducing legislative modifications by summarizing a single CJUE's judgment would further complicate the Court's task by creating additional layers of interpretation, potentially generating uncertainty rather than resolving it. Instead of modifying the definition, we fully support mandating the EDPB to integrate the Court's guidance provided in Case C-413/23 P into forthcoming guidelines. We therefore support the proposed recital 27a as consequence.
~~(28) In order to assess whether research meets the conditions of scientific research for the purpose of this Regulation, account can be taken of elements such as methodological and systematic approach applied while conducting the research in the specific area. Research and technology development should be conducted in academic, industry and other settings, including small and medium-sized undertakings, (Article 179(2) TFEU) and should be always of a of high quality and should adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability).~~	FI (Comments): Finland can support deleting recital 28. However, Finland can show flexibility to continue the discussions on the definition of scientific research (see comments and drafting suggestions below for the definition). If the new definition for scientific research is to be removed from the proposal, Finland considers that the accompanying recitals should be deleted accordingly. IT

Presidency first compromise text	Drafting suggestions and Comments
	(Drafting suggestions): Scientific research and technological development, including research in fields such as biomedical engineering, bionics, neurotechnology, robotics, brain-computer interfaces, advanced prosthetics, organ bioprinting and other emerging technologies, constitute essential components of the freedom of science and innovation protected under Article 13 of the Charter of Fundamental Rights of the European Union. In order to foster innovation, competitiveness and public health, the processing of personal data strictly necessary for such research activities should not be subject to disproportionate regulatory burdens or prior administrative authorisation.
(29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it ~~is not~~**should not be** necessary to ascertain on the basis of Article 6(4) of ~~this~~ Regulation **(EU) 2016/679** whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected. **Such further processing should be considered compatible, provided that it is carried out in compliance with the principle of purpose limitation and subject to appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89. The qualification of processing as being carried out for scientific research purposes should be based on objective characteristics of the research activity and should not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679. In order to assess whether scientific research activities meet the conditions of scientific research for the purpose of Regulation (EU) 2016/679, account can be taken of elements such as the purpose of the research, the methodological approach and ethical standards applied in the specific**	CZ (Drafting suggestions): (29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it ~~is not~~**should not be** necessary to ascertain on the basis of Article 6(4) of ~~this~~ Regulation **(EU) 2016/679** whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected. **Such further processing should be considered compatible, provided that it is carried out in compliance with the principle of purpose limitation and subject to appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89~~. The qualification of processing as being carried out for scientific research purposes should be based on objective characteristics of the research activity and should not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679.~~ In order to assess whether scientific research activities meet the conditions of scientific research for the purpose of Regulation (EU) 2016/679, account can be taken of elements

Presidency first compromise text	Drafting suggestions and Comments
area while conducting the research, and adherence to the principles of transparency, reliability, accountability and oversight, verifiability, and rules for research integrity. Scientific research activities should concur to public interest and well-being, prevent individuals from being subjected to harm or other adverse effects due to participating in scientific research and include – among other things – the respect for human autonomy and the notion of consent to participate in research. Scientific research activities can, amongst others, support innovation such as technology development and may be conducted in academic, industry and other settings, by public authorities or private entities, including small and medium sized undertakings.	**such ~~as the purpose of the research,~~ the methodological approach and ethical standards applied in the specific area while conducting the research, and adherence to the principles of transparency, reliability, accountability and oversight, verifiability, and rules for research integrity. ~~Scientific research activities should concur to public interest and well-being, prevent individuals from being subjected to harm or other adverse effects due to participating in scientific research and include – among other things – the respect for human autonomy and the notion of consent to participate in research.~~ Scientific research activities can, amongst others, support innovation such as technology development and may be conducted in academic, industry and other settings, by public authorities or private entities, including small and medium sized undertakings.** CZ (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	CZ: This is better ensured by providing appropriate definition of "scientific research" in Article 4. CZ: If there is research that has any purpose, it is always research. This should not be put in doubt. CZ: This is partially covered by reference to ethical standards. DK (Drafting suggestions): (29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it ~~is not~~**should not be** necessary to ascertain on the basis of Article 6(4) of ~~this~~ Regulation **(EU) 2016/679** whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected. **Such further processing should be considered compatible, provided that it is carried out in compliance with the principle of purpose limitation and subject to appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89. The**

Presidency first compromise text	Drafting suggestions and Comments
	qualification of processing as being carried out for scientific research purposes should be based on objective characteristics of the research activity and should not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679. ~~**In order to assess whether scientific research activities meet the conditions of scientific research for the purpose of Regulation (EU) 2016/679, account can be taken of elements such as the purpose of the research, the methodological approach and ethical standards applied in the specific area while conducting the research, and adherence to the principles of transparency, reliability, accountability and oversight, verifiability, and rules for research integrity. Scientific research activities should concur to public interest and well-being, prevent individuals from being subjected to harm or other adverse effects due to participating in scientific research and include – among other things – the respect for human autonomy and the notion of consent to participate in research. Scientific research activities can, amongst others, support innovation such as technology development and may be conducted in academic, industry and other settings, by public authorities or private entities, including small and medium sized undertakings.**~~ DK (Comments): DK is opposed to the proposed addition to the preamble, as it, if interpreted too strictly, will risk setting the bar too high for scientific research. DK suggests to either delete the paragraphs beginning with “in order to assess whether” from the proposed addition to the preamble. Alternatively, it could be added to existing text that the definition on scientific research may already come from national law. Furthermore, the reference to consent as a prerequisite should be deleted.

Presidency first compromise text	Drafting suggestions and Comments
	FI (Drafting suggestions): Finland proposes to keep the Commission's original wording. FI (Comments): Finland remains somewhat cautious concerning the compromise proposal to delete the reference to Article 6(4) from the Article 5(1)(b) of the GDPR (see further comments and drafting suggestions below). If the new definition for scientific research is to be deleted, Finland considers that the accompanying recital text should also be deleted.
(30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in various phases in the AI lifecycle, such as the training, testing and validation phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes of a legitimate interest within the meaning of Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.	FI (Drafting suggestions): (30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in various phases in the AI lifecycle, such as the training, testing and validation phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes of a legitimate interest within the meaning of pursuant to Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements, such as data subjects rights, and principles of

Presidency first compromise text	Drafting suggestions and Comments
	that Regulation are met. Public authorities may base the processing of personal data in the context of the development and operation of an AI system for the performance of a task carried out in the public interest pursuant to Article 6, paragraph 1, point (e) and paragraph 2 of Regulation (EU) 2016/679. (31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller, appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, **~~providing an unconditional right to object to the processing of their personal data,~~** respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions. **When the processing is based on point (f) of Article 6(1) of Regulation (EU) 2016/679, the data subject shall also have an unconditional right to object to the processing of their personal data, which goes beyond the right referred in Article 21(1) of that Regulation.** FI

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): Finland proposes the following clarifications based on the EPDB-EDPS Joint Opinion (paras 41-45). Finland proposes the following clarifications based on the EPDB-EDPS Joint Opinion (paras 41-45). **See drafting suggestions striken, bolded and underlined.** **Finland also proposes to clarify the processing carried out by public authorities in the public interest**. It is as vital to ensure that also public authorities may utilise AI to promote public interest and better services and to process personal data in the context of the development and operation of an AI system. Finland underlines that the current wording of the GDPR states that public authorities cannot rely on Article 6(1)(f) of the GDPR in the performance of their tasks. **See drafting suggestion bolded and underlined**. See also comments and drafting suggestions below in Article 88c. NL (Drafting suggestions): ~~(30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in various phases in the AI lifecycle, such as the training, testing and validation phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes of a legitimate interest within the meaning of Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.~~

Presidency first compromise text	Drafting suggestions and Comments
	NL (Comments): NL proposes deletion because of the proposed deletion of the corresponding Article 88c.
(31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller, appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.	FI (Drafting suggestions): (31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller, appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, **~~providing an unconditional right to object to the processing of their personal data,~~** respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions. **When the processing is based on point (f) of Article 6(1) of Regulation (EU) 2016/679, the data subject shall also have an unconditional right to**

Presidency first compromise text	Drafting suggestions and Comments
	object to the processing of their personal data, which goes beyond the right referred in Article 21(1) of that Regulation. FI (Comments): Finland proposes clarifications concerning the unconditional right to object (similarly than EDPB-EDPS Joint Opinion, para 42). Finland also welcomes the Presidency to come up with a solution to clarify what "enhanced transparency" means (see EDPB-EDPS Joint Opinion, para 43). NL (Drafting suggestions): ~~(31) When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller, appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to~~

Presidency first compromise text	Drafting suggestions and Comments
	~~effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.~~ NL (Comments): NL proposes deletion because of the proposed deletion of the corresponding Article 88c.
(32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research ~~therefore pursues a~~**may be necessary for the purposes of the** legitimate ~~interest~~**interests pursued by a controller or by a third-party** within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State **law. Scientific research can also follow public interest and be based on Member States and Union** law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.	CZ (Drafting suggestions): (32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research **therefore pursues a ~~may be necessary for the purposes of the~~** legitimate **interest ~~interests~~ pursued by a controller or by a third-party** within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State **law. Scientific research can also follow public interest and be based on Member States and Union** law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met. CZ (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	  CZ: As this recital concerns the legal basis under Article 6(1)(f) GDPR and explicitly refers to all other requirements and principles of GDPR, it is confusing to invoke those requirements and principles anyway. FI (Drafting suggestions): (32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research therefore pursues **may be necessary for the purposes of the** legitimate ~~interest~~**interests pursued by a controller or by a third-party** within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State **law. The processing of personal data for the purpose of s~~S~~cientific research can also follow public interest and be based on Member States and Union law**. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met. FI

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): Finland supports that the Presidency has clarified that processing personal data for scientific research can also follow from public interest and Member State/Union law. Finland has a technical comment (see drafting suggestion bolded and underlined) NL (Drafting suggestions): Small clarification in the penultimate sentence: Scientific research can also follow public interest **as meant in Article 6(1)(e) of Regulation (EU) 2016/679** and be based on Member States and Union law.
	IT (Drafting suggestions): **(32a)** In applying Regulation (EU) 2016/679, due regard shall be given to the need to ensure a fair balance between the right to the protection of personal data and other fundamental rights and freedoms guaranteed by the Charter of Fundamental Rights of the European Union, including the freedom to conduct a business (Article 16), the freedom of the arts and sciences (Article 13), the freedom of expression and information (Article 11), and the right to property (Article 17). Enforcement and interpretation of this Regulation shall ensure that such rights are afforded equal constitutional consideration in accordance with the principles of proportionality and practical concordance.
(33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing. In order not to disproportionately	FI (Drafting suggestions): (33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may residually exist in

Presidency first compromise text	Drafting suggestions and Comments
hinder the development and operation of AI and taking into account the capabilities of the controller to identify and remove special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle of an AI system or AI model and, once it identifies such data, effectively remove them. If removal would require disproportionate effort, notably where the removal of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, the controller should effectively protect such data from being used to infer outputs, being disclosed or otherwise made available to third parties. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679.	the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing. In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and remove special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed **for incidental and residual processing of special categories of data in the context of the development of AI systems or models. The derogation should not be understood as covering the processing of special categories of personal data collected through prompts during the deployment of the AI system or model**. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle of an AI system or AI model and, once it identifies such data, effectively remove them. If **removal is not possible or** would require disproportionate effort, notably where the removal of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, the controller should effectively protect such data **from being used for other purposes**, being used to infer outputs, being disclosed or otherwise made available to third parties. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679. **This derogation shall be without prejudice to the application of Article 4a of Regulation (EU) 2024/1689 that provides a legal ground for processing special categories of data for the purpose of ensuring bias detection and correction in the context of AI systems**. FI (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	Finland proposes to clarify the scope of the proposed derogation for incidental and residual processing of special categories of data (see EDPB-EDPS Joint Opinion paras 48-52). **See drafting suggestions bolded and underlined. See also comments and drafting suggestions for the Article text below**. NL (Drafting suggestions): ~~(33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing. In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and remove special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle of an AI system or AI model and, once it identifies such data, effectively remove them. If removal would require disproportionate effort, notably where the removal of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, the controller should effectively protect such data from being used to infer outputs, being disclosed or otherwise made available to third parties. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679.~~

Presidency first compromise text	Drafting suggestions and Comments
	NL (Comments): NL proposes deletion because of the proposed deletion of the corresponding Article 9(2)(k).
(34) **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric data includes two distinct functions, namely the identification of a natural person or the verification (also called authentication) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary **and proportionate** for a purpose pursued by the controller~~,~~ and **when provided for under Union or Member States law. The controller should choose from equally effective means the less intrusive one. This derogation should apply where** suitable safeguards apply to ~~enable the data subject to have sole control of~~**ensure that the biometric data or the means needed for** the verification ~~process~~**are under the sole control and possession of the data subject**. For example, **this is the case** where the biometric data are securely stored solely at the ~~side~~**device** of the data subject or are securely stored ~~at the side of~~**by** the controller in a	BE (Drafting suggestions): (34) **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of ~~biometric data~~ **<u>biometric recognition</u>** includes two distinct functions, namely the identification of a natural person or the verification (also called authentication) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary **and proportionate** for a purpose pursued by the controller~~,~~ and **when provided for under Union or Member States law. The controller should choose from equally effective means the less intrusive one. <u>Where biometric</u>**

Presidency first compromise text	Drafting suggestions and Comments
state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, ~~that~~**and subject to measures ensuring the overall security of** processing ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~**, including during the enrolment phase of data subject's** biometric data ~~or only for a very limited time~~**and** during the verification process.	**data are processed for the purpose of confirming the identity of a data subject, controllers should, where possible, prioritise authentication methods that do not involve the processing of biometric data. The processing of biometric data for identity verification should therefore only be used where necessary and proportionate and subject to appropriate safeguards. For the purposes of this Regulation, biometric identification should be understood as the processing of biometric data through comparison against a database intended to determine the identity of a natural person, whereas biometric verification refers to a one-to-one comparison used solely to confirm a claimed identity.** **This derogation should apply where** suitable safeguards apply to ~~enable the data subject to have sole control of~~**ensure that the biometric data or the means needed for** the verification ~~process~~**are under the sole control and possession of the data subject**. For example, **this is the case** where the biometric data are securely stored solely at the ~~side~~**device** of the data subject or are securely stored ~~at the side of~~**by** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, ~~that~~**and subject to measures ensuring the overall security of** processing ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~**, including during the enrolment phase of data subject's** biometric data ~~or only for a very limited time~~**and** during the verification process. **Such verification may in particular be required in the context of electronic identification systems and trust services under Union law.** BE (Comments): This clarification aims to ensure legal certainty regarding the distinction between biometric identification (one-to-many comparison) and biometric verification (one-to-one comparison used to confirm a claimed identity). In practice, several authentication solutions, including those used in electronic

Presidency first compromise text	Drafting suggestions and Comments
	identification systems and digital wallets, rely on one-to-one verification where the biometric data remain under the control of the user. Clarifying this distinction in the recital could help avoid divergent interpretations of Article 9 across Member States while maintaining the existing level of protection. Necessity and proportionality tests must remain stringent, and the "less intrusive alternative" requirement should be maintained. CZ (Drafting suggestions): (34) **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric data includes two distinct functions, namely the identification of a natural person or the verification (also called authentication) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary ~~**and proportionate**~~ for a purpose pursued by the controller~~,~~ and ~~**when provided for under Union or Member States law**~~**. The controller should choose from equally effective means the less intrusive one. This derogation should apply where** suitable safeguards apply to ~~enable the data subject to have sole control of~~**ensure that the biometric data or the means needed for** the verification ~~process~~**are under the sole control and possession of the data subject**. For example, **this is the case** where the biometric data are securely stored solely at the ~~side~~**device** of the data subject or are securely stored ~~at the side of~~**by** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is

Presidency first compromise text	Drafting suggestions and Comments
	securely held solely by the data subject, ~~that~~**and subject to measures ensuring the overall security of** processing ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~**, including during the enrolment phase of data subject's** biometric data ~~or only for a very limited time~~**and** during the verification process. CZ (Comments): CZ: CZ is against the words "and proportionate" which are not used in Art. 9(2) in relation to processing. Given the narrowly defined use case, doubts about proportionality are unfounded and counter-productive.

Presidency first compromise text	Drafting suggestions and Comments
	CZ is against the necessity to adopt EU or domestic legislation for the mere verification that is practically under sole control of data subject. Appropriate safeguard is already provided by the provision itself. This would essentially force Member States to design unnecessary legislative burdens that would only prevent free flow of European verification solutions. If a Member State identifies a grave need to require such safeguards, relevant legislation can be adopted under Art. 9(4) GDPR in its current wording. DK (Comments): DK prefers the Commission's proposal to avoid the risk for fragmentation. FI (Drafting suggestions): (34) **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric data includes two distinct functions, namely the identification of a natural person or the verification (also called authentication) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary **and proportionate** for a purpose pursued by the controller~~,~~ and **when provided for under Union or Member States law. The controller should choose from equally effective means the less intrusive ones and provide the data subject equally effective and less**

Presidency first compromise text	Drafting suggestions and Comments
	intrusive means for the verification process. This derogation should apply where suitable safeguards apply to ~~enable the data subject to have sole control of~~**ensure that the biometric data or the means needed for** the verification ~~process~~**are under the sole control and possession of the data subject**. For example, **this is the case** where the biometric data are securely stored solely at the ~~side~~**device** of the data subject or are securely stored ~~at the side of~~**by** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, ~~that~~**and subject to measures ensuring the overall security of** processing ~~is not~~ data subject's biometric data and during the verification process. FI (Comments): Finland welcomes the Presidency's efforts to ensure appropriate safeguards and proportionality of processing biometric data and supports the clarifications made in recital 34. Finland proposes that the recital 34 would clearly state that the controller should leave the data subject a possibility to choose between equally effective and less intrusive means (i.e., the controller does not limit the possibility only to biometric verification when there are other means for verification). **See drafting suggestion bolded and underlined**. However, Finland remains cautious whether Member State/Union law is the best way forward and proposes to delete this from Article (9(2)(l) as well as from recital 34 (see also comments below). NL (Drafting suggestions): (34) **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or

Presidency first compromise text	Drafting suggestions and Comments
	confirms the unique identification of that person. The notion of biometric data includes two distinct functions, namely the identification of a natural person or the verification (~~also called authentication~~ as defined in Article 3(36) of Regulation (EU) 2024/1689, which includes authentication) of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of Regulation **(EU) 2016/679** should be allowed where the verification of the claimed identity of the data subject is necessary **and proportionate** for a purpose pursued by the controller~~, and when provided for under Union or Member States law~~**.** The controller should choose from equally effective means the less intrusive one. This derogation should apply where **appropriate** ~~suitable~~ safeguards apply to ensure that the biometric data or the means needed for the verification are under the sole control and possession of the data subject. For example, this is the case where the biometric data are securely stored solely at the device of the data subject or are securely stored by the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is securely held solely by the data subject, and subject to measures ensuring the overall security of processing including during the enrolment phase of data subject's biometric data and during the verification process. **Other examples of appropriate safeguards are ensuring that end-to-end encryption is used when data are transmitted over a communication channel and providing data subjects with the possibility to securely delete their biometric data at any time.** NL (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	- NL proposes to clarify that the definition of biometric verification is to be interpreted in the same way as the definition of biometric verification in Article 3(36) of the AI Act, which includes authentication. - Furthermore, NL proposes deletion of the requirement regarding Union of Member States law, because of the proposed deletion of the corresponding reference in Article 9(2)(l). - Following the EDPB/EDPS opinion on this proposal (§38 and footnote 45), NL proposes to add some examples of appropriate safeguards that controllers should implement when processing biometric data for verification purposes.
(35) Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain **confirmation** from the controller~~ confirmation~~ as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. ~~By contrast, it should be clarified in~~ Article 12 **(5) of that**~~of the~~ Regulation **already provides that where the request to exercise**~~that~~ the right of access~~, which is from the outset favourable to data subjects,~~ **is manifestly unfounded or excessive, the controller may either charge a reasonable fee or refuse to act on the request. It is important to clarify that this** should ~~not be abused in the sense that~~**apply also where an abusive intention on the part of** the data ~~subjects abuse them for purposes other than the protection of their data~~**subject submitting those requests can be demonstrated by the controller**. For example, such an ~~abuse of the right of access~~**abusive intention** would arise where the data subject ~~intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make~~**submits** excessive ~~use of the right of access~~**numbers of identical or largely similar**	FI (Comments): Finland supports in principle the proposed changes that clarify the proposal on manifestly unfounded/excessive request. Finland does not support limiting the right under Article 15 of the GDPR as it would weaken the current level of data protection and would go against the objective of the whole Digital Omnibus proposal. NL (Comments): If the addition to Article 12(5) would be extended from data access requests to all data subject requests following the amendment of NL on that provision, then recital 35 should be extended to all data subject requests as well.

Presidency first compromise text	Drafting suggestions and Comments
requests with the ~~only~~**sole** intent of causing damage or harm to the controller**. Another example of abusive intention includes situations** ~~or~~ when an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller. ~~Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of proof regarding the excessive character of a request than regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character of a request concerns the possibly abusive conduct of a data subject, which lies primarily outside the controller's sphere of influence, and therefore the controller may be able to prove such abuse only to a reasonable level. In any event, while requesting access under Article 15 of Regulation (EU) 2016/679 the data subject should be as specific as possible. Overly broad and undifferentiated requests should also be regarded as excessive.~~	
(36) Article 13 of Regulation (EU) 2016/679 requires the data controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of data controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of ~~the~~**that** Regulation, this derogation should be extended to situations where the processing is not likely to result in a high risk, within the meaning of Article 35 of ~~the~~**that** Regulation, and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 **of Article 13** in the light of the context in which the personal data have been collected, in particular regarding the relationship between data subjects and	DK (Drafting suggestions): 36) Article 13 of Regulation (EU) 2016/679 requires the data controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of data controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of ~~the~~**that** Regulation, this derogation should be extended to situations where the processing is not likely to result in a high risk, within the meaning of Article 35 of ~~the~~**that** Regulation, and there are reasonable grounds to assume that the data subject

Presidency first compromise text	Drafting suggestions and Comments
the controller. **The application of the derogation from the information obligation should not undermine the principle of transparency and should be limited to situations where the controller can objectively demonstrate that the data subject already possesses the required information.** These should be the situations where the **personal data are collected in the** context of ~~the~~**a direct, limited and clearly circumscribed** relationship between ~~the~~**data subjects and a** controller and ~~the data subject is very clear and circumscribed and the controller's activity is not data-intensive~~**does not involve the processing of a large amount of personal data**, such as the relationship between a craftsman and their clients, where the scope of processing is limited to the minimum data necessary to perform the service~~. The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment. In such circumstances, that is to say when the processing is non data-intensive, non-complex and where the controller collects a low amount of personal data, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller as well as on the purpose of the processing when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679~~. The same should apply to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the	already has the information referred to in points (a) and (c) of paragraph 1 **of Article 13** in the light of the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller. **The application of the derogation from the information obligation should not undermine the principle of transparency ~~and should be limited to situations where the controller can objectively demonstrate that the data subject already possesses the required information~~.** These should be the situations where the **personal data are collected in the** context of ~~the~~**a direct, limited and clearly circumscribed** relationship between ~~the~~**data subjects and a** controller and ~~the data subject is very clear and circumscribed and the controller's activity is not data-intensive~~**does not involve the processing of a large amount of personal data**, such as the relationship between a craftsman and their clients, where the scope of processing is limited to the minimum data necessary to perform the service~~. The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment. In such circumstances, that is to say when the processing is non data-intensive, non-complex and where the controller collects a low amount of personal data, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller as well as on the purpose of the processing when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679~~. The same should apply to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. Where the derogation from the obligations of Article 13 does not apply, in order to

Presidency first compromise text	Drafting suggestions and Comments
information required, notably by allowing users to navigate to further information.	balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information. DK (Comments): DK suggests to delete the obligation that the controller must be able to "objectively demonstrate", as this could be understood as requiring some sort of documentation made by small businesses. FI (Comments): Finland supports the proposed amendments. NL (Drafting suggestions): Small clarification in the 6th sentence: The same should**, under the under the aforementioned conditions,** apply to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities.
(37) Where the **further** processing **by the same controller** takes place for the purpose of scientific research and the provision of information to the data subject proves to be impossible or would involve a disproportionate effort it should not be necessary to provide the information provided for under Article 13 of this Regulation. The controller should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort. The provision of the information would involve a disproportionate effort in particular where the controller at the time	DK (Drafting suggestions): 37) Where the ~~**further**~~ processing ~~**by the same controller**~~ takes place for the purpose of scientific research and the provision of information to the data subject proves to be impossible or would involve a disproportionate effort it should not be necessary to provide the information provided for under Article 13 of this Regulation. The controller should make reasonable efforts to

Presidency first compromise text	Drafting suggestions and Comments
of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects. In such situations the controller should inform data subjects indirectly, such as by making the information publicly available. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information publicly available should be determined depending on the context of the research project and the data subjects involved.	acquire contact details if they are readily available and acquisition would not require a disproportionate effort. The provision of the information would involve a disproportionate effort in particular where the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects. In such situations the controller should inform data subjects indirectly, such as by making the information publicly available. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information publicly available should be determined depending on the context of the research project and the data subjects involved. DK (Comments): DK does not support the proposed limitation of when the exemption from the obligation to provide information applies in relation to scientific research. As we see it, it should also apply to disclosure as it was originally proposed. If the exemption cannot cover disclosure, the obligation to provide information will be used as a justification for not sharing information with relevant scientific research studies. This will hinder the exchange of data, and thus the possibility of introducing innovative solutions.
~~(38) Article 22 of Regulation (EU) 2016/679 provides for rules governing the processing of personal data when the data controller makes decisions which have legal effects or similarly significant effects on the data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified that decisions based solely on automated processing are allowed when specific conditions are met, as set out in~~	CZ (Drafting suggestions): **(38) Article 22 of Regulation (EU) 2016/679 provides for rules governing the processing of personal data when the data controller makes decisions which have legal effects or similarly significant effects on the**

Presidency first compromise text	Drafting suggestions and Comments
~~Regulation (EU) 2016/679. It should also be clarified that when assessing whether a decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. This means that the fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing When several equally effective automated processing solutions exist, the controller should use the less intrusive one.~~	**data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified** ~~that decisions based solely on automated processing are allowed when specific conditions are met, as set out in Regulation (EU) 2016/679. It should also be clarified~~ **that when assessing whether a decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. This means that the fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing When several equally effective automated processing solutions exist, the controller should use the less intrusive one.** CZ (Comments): CZ: CZ agrees with the Presidency that the right not to be subject to automated decisions and the fundamental structure of Article 22 should be maintained, but in order to simplify conditions for development of European digital economy, finds it advisable and beneficial to clearly enable automated decision-making online in the context of preparation and conclusion of contracts. FI (Drafting suggestions): (38) Article 22 of Regulation (EU) 2016/679 provides for rules governing the processing of personal data when the data controller makes decisions which have legal effects or similarly significant effects on the data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified ~~that decisions based solely on automated processing are allowed when specific conditions are met, as set out in Regulation (EU) 2016/679. It should also be clarified~~ that when assessing whether a decision is necessary for entering into, or performance of, a

Presidency first compromise text	Drafting suggestions and Comments
	contract between the data subject and a data controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. This means that the fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing When several equally effective automated processing solutions exist, the controller should use the less intrusive one. FI (Comments): Finland can show flexibility and continue discussions on the Commission's proposal to amend Article 22 GDPR. Finland considers that this Digital Omnibus package should clarify the application of Article 22(2)(a) GDPR. Therefore, Finland proposes the following; we could keep most parts of the proposed recital 38 but remove the text concerning the structural change of Article 22 GDPR. Finland underlines that the EDPB-EDPS Joint opinion was not against clarifying the application of Article 22(2)(a) GDPR
(39) In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation. In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article	NL (Drafting suggestions): (39) In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be **more** aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation. In the case of a data breach that is not likely to result in a**n** **impactful** ~~high~~ risk to the rights and freedoms of natural persons, the controller should not be

Presidency first compromise text	Drafting suggestions and Comments
33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should ~~prepare~~**establish and make public** a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person~~. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption~~**, as well as a common list of circumstances in which a personal data breach does not result in such a high risk**. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. **The alignment of notification thresholds does not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) and Article 30 of Regulation (EU) 2016/679.**	required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should establish and make public a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a**n impactful** ~~high~~ risk to the rights and freedoms of a natural person, as well as a common list of circumstances in which a personal data breach does not result in such a ~~high~~ risk. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in a**n impactful** ~~high~~ risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. The alignment of notification thresholds does not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) and Article 30 of Regulation (EU) 2016/679. NL (Comments): NL proposes these changes to align this recital with the proposed changes from NL to the corresponding Article 33.
(40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that	CZ (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be ~~prepared~~**established and made public** by the Board ~~and adopted by the Commission as an implementing act~~. In order to facilitate compliance by controllers, the Board should also ~~prepare~~**establish and make public** a common template and a common methodology for conducting data protection impact assessments~~, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption~~. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary.	(40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be ~~prepared~~**established and made public** by the Board ~~and adopted by the Commission as an implementing act~~. In order to facilitate compliance by controllers, the Board should also ~~prepare~~**establish and make public** a common template and a common methodology for conducting data protection impact assessments~~, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption~~. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary. **In addition, national supervisory authorities should be able to develop national compatible lists to address local, specific or emerging issues. Such lists should be notified to Board to ensure they remain compatible with EU-wide lists.** CZ

Presidency first compromise text	Drafting suggestions and Comments
	(Comments):

Presidency first compromise text	Drafting suggestions and Comments
	  CZ: CZ supports EU-wide lists and is flexible as regards the competences of Commission or the Board. However, complementary national lists should be possible to address local, specific or emerging issues. These lists should be reported to Board to ensure compatibility with EU-wide lists.
(41) Regulation (EU) 2018/1725 of the European Parliament and of the Council[2] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Directive (EU) 2016/680 of the European Parliament and of the Council[3] applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Regulation (EU) 2018/1725 and Directive (EU) 2016/680 should be brough into alignment with the amendments to Regulation (EU) 2016/679 introduced by this Regulation. 2 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).	

Presidency first compromise text	Drafting suggestions and Comments
3 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).	
(42) As clarified in recital 5 of Regulation (EU) 2018/1725, whenever the provisions of Regulation (EU) 2018/1725 follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union, be interpreted homogeneously. The scheme of Regulation (EU) 2018/1725 should be understood as equivalent to the scheme of Regulation (EU) 2016/679. Therefore, this Regulation also amends the provisions of Regulation (EU) 2018/1725 that are concerned by the amendments of Regulation (EU) 2016/679, insofar as the latter amendments are also relevant in the context of the processing of personal data by the Union institutions, bodies, offices and agencies.	
(43) In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Directive (EU) 2016/680 and any other Union legal act applicable to such processing of personal data should follow after the adoption of this regulation, in order to allow for their application as close as possible to the entry into application of the amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.	
(44) The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely Regulation (EU) 2016/679, where the subscriber of the electronic	FI (Comments):

Presidency first compromise text	Drafting suggestions and Comments
communications service or the user of the terminal equipment is a natural person. The amendments presented in this Regulation continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. The relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.	Finland has previously commented on the "the subsequent processing" and welcomes the Presidency to consider the EDPB-EDPS Joint Opinion (paras 99-100).
The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment should continue to be allowed only on the basis of consent. Similar to the approach in Directive 2002/58/EC, this requirement should not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, when that is based on Union or Member State law within the meaning of Article 6 of Regulation (EU) 2016/679 and if it fulfils all conditions of lawfulness laid down in that provision, and is done for the objectives laid down in Article 23(1) of Regulation (EU) 2016/679.	NL (Drafting suggestions): The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment should continue to be allowed only on the basis of consent. Similar to the approach in Directive 2002/58/EC, this requirement should not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, when that is based on Union or Member State law within the meaning of Article 6 of Regulation (EU) 2016/679 and if it fulfils all conditions of lawfulness laid down in that provision, and is done for the objectives laid down in Article 23(1) of Regulation (EU) 2016/679**, under the conditions laid down in Article 23(2)**. NL (Comments): NL proposes this addition to align this recital with the proposed shift of the corresponding Article 88a(2) to Article 23 of the current GDPR.
With a view to reducing the compliance burden and providing legal clarity to controllers, and given that certain purposes of processing pose a	FI

Presidency first compromise text	Drafting suggestions and Comments
low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by the data subject, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, this Regulation should therefore provide that the processing is lawful. The controller, such as a media service provider, may mandate a processor, such as a market research company, to carry out the processing on its behalf.	(Drafting suggestions): With a view to reducing the compliance burden and providing legal clarity to controllers, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by the data subject, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, this Regulation should therefore provide that the processing is lawful. **Such lawful processing should include the use of functional cookies that enhance the usability of the service, such as cookies used to limit the number of times certain content is shown to a user.** The controller, such as a media service provider, may mandate a processor **or joint controller**, such as a market research company **and Joint Industry Committee**, to carry out the processing **jointly or** on its behalf. **The requirement that the processing is solely for their own use does not prevent the controller or joint controller from sharing the resulting aggregated information about the service's audiences.** FI (Comments): First, Finland supports the aim of the proposal to reduce cookie fatigue. To ensure that this is reached, Finland suggests that additional low-risk purposes for the use of cookies without consent are explored. In addition, the proposal requires further clarification to ensure that the obligations on service providers are clear and feasible. The Commission's proposal deviates from the requirement of ePrivacy directive, as the proposal does not require for the purpose to be *strictly necessary* for the white-listed grounds, as storing of and gaining access to

Presidency first compromise text	Drafting suggestions and Comments
	personal data in the terminal equipment would be lawful to the extent it is *necessary* for the specific grounds. Finland welcomes this adjustment, as this could bring more flexibility to the interpretation of "necessary cookies". Second, please see justification under 88a(3). Finland has previously commented on the "the subsequent processing" and welcomes the Presidency to consider the EDPB-EDPS Joint Opinion (paras 99-100). NL (Drafting suggestions): With a view to reducing the compliance burden and providing legal clarity to controllers, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by the data subject, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, this Regulation should therefore provide that the processing is ~~lawful~~ **permissible where it is based upon a legal basis in accordance with Article 6(1) other than consent**. The controller, such as a media service provider, may mandate a processor, such as a market research company, to carry out the processing on its behalf. NL (Comments): NL proposes this change to align this recital with the proposed changes to the corresponding Article 88a(3).

Presidency first compromise text	Drafting suggestions and Comments
For the subsequent processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied. It is the responsibility of the controller in the light of the principle of accountability to choose the appropriate legal basis for the intended processing. In order to be able to rely on legitimate interest under Article 6(1), point f, of Regulation (EU) 2016/679 as a ground for the subsequent processing of personal data, the controller must show that it pursues the controller's or third parties' legitimate interest, the processing is necessary in order to achieve the purpose of that legitimate interest, and the interests or fundamental rights of the data subject do not override the interests pursued by the controller. In this context, controllers should take outmost account of the following elements: whether the data subject is a child; the reasonable expectations of data subject; the impact on the individual either because of the scale of data processed or the sensitivity of the data processed; the scale of the processing at issue in the sense that the processing cannot be particularly extensive either because of their amount or the range of categories of data; the processing should be based on data limited to what is necessary and cannot be based on monitoring of large parts of the online activity of the data subjects; and other relevant factors as appropriate. The processing should not give rise to the continuous monitoring of the data subject's private life.	FI (Comments): Finland has previously commented on the "the subsequent processing" and welcomes the Presidency to consider the EDPB-EDPS Joint Opinion (paras 99-100).
Where the controller cannot rely on legitimate interest as a legal ground for the subsequent processing, the processing should be based on another ground in Article 6(1), in particular on consent in accordance with Articles 6 and 7 of Regulation (EU) 2016/679, provided that all principles of Regulation (EU) 2016/679 are met.	FI (Comments): Finland has previously commented on the "the subsequent processing" and welcomes the Presidency to consider the EDPB-EDPS Joint Opinion (paras 99-100).
(45) Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the	FI (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
data subjects which may consent just in order to avoid repeating requests. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period.	**Dark patterns in cookie banners are problematic as they manipulate users into making choices that are not genuinely voluntary or informed. To tackle the use of problematic consent requests, the data subjects shall be able to refuse requests in a user-friendly manner. However, this does not preclude the possibility of the service provider to inform the user of the use of cookies.** Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the data subjects which may consent just in order to avoid repeating requests. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period. **However, the controller may request consent within the period if the development of the service, a change in the purpose of processing, or another comparable and justified reason makes a renewed request necessary. The regulation does not require the service provider to attempt to identify the user for a six-month period if the cookie or other technology is no longer valid for reasons beyond the service provider's control, such as when the user has deleted the cookies or similar identifiers.** FI (Comments): Finland supports the proposed rule that new consent should not be requested within 6 months of the users' refusal to give consent. However, there are some situations, where new consent requests could be considered justified. These require further clarification and could be done with few additions to the recitals. First, the service provider may develop its service and change the purposes for which access and use of information on the users' terminal equipment within the 6 months period. In such cases there is a legitimate ground for the service provider to request new consent for the updated processing purposes.

Presidency first compromise text	Drafting suggestions and Comments
	Second, the regulation should not require the service provider to try to identify and track users in cases where the users have cleared and deleted the cookies. NL (Drafting suggestions): (45) Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the data subjects which may consent just in order to avoid repeating requests. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period. **This obligation is applicable to any controller that accesses or stores personal data in the terminal equipment of the data subject, including third party cookie providers.** NL (Comments): In accordance with §111 of the EDPB/EDPS Opinion, NL proposes to clarify this recital.
(46) Data subjects should have the possibility to rely on automated and machine-readable indications of their choice to consent or refuse a consent request or object to the processing of data. Such means should follow the state of the art. They can be implemented in the settings of a web browser or in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation should support the emergence of market-driven solutions with appropriate interfaces. The controller should be obliged to respect automated and machine-readable indications of data subject's choices once there are available standards. In light of the importance of independent journalism in a democratic society and	FI (Drafting suggestions): --- In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices. **This exemption should also cover situations in which media service providers rely on technologies supplied by external partners, such as cookies or similar tools placed by such partners, for the delivery of advertising, audience measurement or**

Presidency first compromise text	Drafting suggestions and Comments
in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices. The obligation for providers of web browsers to provide the technical means for data subjects to make choices with respect to the processing should not undermine the possibility for media service providers to request consent by data subjects.	**other functionalities necessary for the sustainable provision of media services.** FI (Comments): Finland welcomes the Commission's proposal to exclude media service providers from the centralised consent regime. The proposal recognises the importance of digital advertisement revenues for independent journalism as an indispensable pillar of a democratic society. To fully realise the benefits of the media exemption, it should be clarified that the exemption also covers third-party cookies when used in connection with media services.
(47) Directive 2002/58/EC on privacy and electronic communications 'ePrivacy Directive'), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of user's or subscriber's terminal equipment used for such communications. The current provision of Article 5(3) of Directive 2002/58/EC should remain applicable insofar as the subscriber or user is not a natural person, and the information stored or accessed does not constitute or lead to the processing of personal data.	
(48) Article 4 of Directive 2002/58/EC should be repealed. Article 4 of Directive 2002/58/EC sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements. Subsequently, Directive (EU) 2022/2555 has set new requirements as regards cybersecurity risk-management measures and incident reporting for those providers. In order to reduce overlapping obligations for entities in the electronic communications sector, Article 4 of Directive 2002/58/EC should be repealed. As regards the security of processing of personal data pursuant to Article 4(1) and (1a) of	

Presidency first compromise text	Drafting suggestions and Comments
this directive and the notification of personal data breaches pursuant to Article 4(3) to (5) of Directive 2002/58/EC this directive, the Regulation (EU) 2016/679 already provide for comprehensive and up-to-date rules. These rules should therefore apply to providers of publicly available electronic communication services and providers of public communications networks, thereby ensuring that one regime applies to the controllers and processors.	
(58) The European Data Protection Supervisor ~~was~~**and the European Data Protection Board were** consulted in accordance with Article ~~42(1)~~**42** of Regulation (EU) 2018/1725 of the European Parliament and of the Council[4], and delivered ~~its~~**their joint** opinion on ~~[DATE]. The European Data Protection Board was consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on [DATE]~~**10 February 2026**. 4 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).	
(59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 provide a comprehensive regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms,	BE (Drafting suggestions): (59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 provide a ~~comprehensive~~ regulatory framework for a safe, predictable and trusted online environments

Presidency first compromise text	Drafting suggestions and Comments
and given that the objectives and material provisions of the Platform-to-Business Regulation are largely covered by the Digital Services Act and the Digital Markets Act, Regulation (EU) ~~2019/1050~~**2019/1150** should be repealed. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty **and for purposes of keeping the necessary level of protection for business users**, selected definitions in Article 2, the provisions on restrictions and suspensions in Article 4, as well as on the internal complaint-handling system in Article 11 of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, **or that are not covered by other legal acts,** in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and Article 15 ensuring enforcement, will temporarily remain in application until ~~the original acts are amended.~~**2032.**	for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that **some** objectives and material provisions of the Platform-to-Business Regulation are ~~largely~~ covered by the Digital Services Act and the Digital Markets Act, Regulation (EU) ~~2019/1050~~**2019/1150** should be **partially** repealed. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty **and of keeping the necessary level of protection for business users**, ~~selected definitions in~~ **Articles 2, points (1) to (10) and (13), 3, 4, 5, 7, 10, 11 and 15 should remain in application as they contain obligations that are not fully covered by Regulations (EU) 2022/2065 and (EU) 2022/1925.** ~~the provisions on restrictions and suspensions in Article 4, as well as on the internal complaint-handling system in Article 11 of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, **or that are not covered by other legal acts,** in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and Article 15 ensuring enforcement, will temporarily remain in application until the original acts are amended.~~**2032.** BE (Comments): While Belgium acknowledges and supports the Commission's efforts to reduce administrative burdens by avoiding potential overlaps between the P2B Regulation and other EU legislation. Addressing those parts of the P2B Regulation that clearly overlap with other EU legislation, primarily the DSA and DMA, will simplify the applicable rules and increase legal certainty for businesses, making the EU more competitive and commercially attractive.

Presidency first compromise text	Drafting suggestions and Comments
	However, the Commission's proposal to repeal the entire P2B Regulation, with only limited and time-gated exceptions, will lead to loopholes and weaknesses in the legal protections, that are disproportionate to the marginal reduction in administrative burdens that would be achieved. While simplification efforts are supported, they should not come at the expense of the essential safeguards for European SMEs. Such safeguards include transparency regarding general terms and conditions, predictability in the event of changes, insight into rankings and clear procedures in the event of restriction or suspension. Their importance is reflected in the growing awareness of P2B rights and the increasing number of complaints concerning non-compliant platforms. The P2B Regulation contributes to the proper functioning of the single market by harmonising rules that afford transparency, fairness and effective redress tools to business users of platforms. In this regard, it has a specific approach and constitutes a first step toward establishing a comprehensive EU legal framework for online intermediaries. The DMA and DSA have different targets and scopes. They do not provide the same substantive obligations, nor do they offer the subsidiarity and proximity afforded by the P2B Regulation. Therefore, they cannot offer the same level of protection in such situations. Simplification efforts should lead to a genuine reduction in regulatory burden. We believe that targeted adjustments to remove clear overlaps with the DSA and DMA would streamline the regulatory framework without dismantling essential protections. The limited administrative burden associated with the remaining P2B provisions, would be proportionate in light of the legal certainty and protection they afford SMEs. Therefore, we propose to maintain certain essential P2B provisions on a permanent basis, while repealing the rest. This partial repeal reflects a more

Presidency first compromise text	Drafting suggestions and Comments
	targeted and proportionate approach to reduce complexity and administrative burdens within the P2B Regulation while preserving the necessary protection this legislation offers for businesses, in particular SMEs. IE (Drafting suggestions): Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 provide a comprehensive regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that the objectives and material provisions of the Platform-to-Business Regulation are largely covered by the Digital Services Act and the Digital Markets Act, Regulation (EU) ~~2019/1050~~ 2019/1150 should be repealed **save for the following provisions: Article 2, Article 3, Article 4, Article 11, Article 12 and Article 15.** Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty and for purposes of keeping the necessary level of protection for business users, ~~selected definitions in~~ Article 2, Article 3~~(2)~~ , ~~Terms and Conditions, the provisions on restrictions and suspensions in~~ Article 4, ~~as well as~~ Article 11, ~~Internal complaint-handling system and~~ Article 12 ~~Mediation, that are not covered in other legal acts,~~ and Article 15 on enforcement of Regulation (EU) 2019/1150, should remain applicable ~~until such time as equivalent protections are expressly provided for in other Union legal acts and the relevant amending measures have entered into force.~~ IE

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): While the Digital Services Act and the Digital Markets Act introduce significant horizontal obligations for providers of intermediary services and gatekeepers, their objectives and material provisions do not fully replicate all safeguards established under Regulation (EU) 2019/1150, notably those relating to advance notice of changes to terms and conditions, transparency of restrictions and suspensions, and access to effective and proportionate dispute resolution mechanisms for business users, including small and micro-enterprises. In the interest of simplification of Union legislation, any repeal or modification of Regulation (EU) 2019/1150 should therefore be accompanied by the retention or explicit replacement of those provisions that are not otherwise covered by Union law, in order to maintain an equivalent level of protection for business users and avoid the dilution of existing rights. IT (Drafting suggestions): (59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 provide a comprehensive regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that **some** objectives and material provisions of the Platform-to-Business Regulation are largely covered by the Digital Services Act and the Digital Markets Act, Regulation (EU) 2019/1150 should be **partially** repealed. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the

Presidency first compromise text	Drafting suggestions and Comments
	requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty and for purposes of keeping the necessary level of protection for business users, selected definitions in **Articles 2, points (1) to (10) and (13), 3, 4, 5, 7, 10, 11, 15 and 19 should remain in application as they contain obligations that are not fully covered by Regulations (EU) 2022/2065 and (EU) 2022/1925.** the provisions on restrictions and suspensions in Article 4, as well as on the internal complaint-handling system in Article 11 of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, **or that are not covered by other legal acts,** in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and Article 15 ensuring enforcement, will temporarily remain in application until the original acts are amended.**2032.** IT (Comments): ITALY acknowledges and supports the Commission's efforts to reduce administrative burdens by avoiding potential overlaps between the P2B Regulation and other EU legislation. Addressing those parts of the P2B Regulation that clearly overlap with other EU legislation, primarily the DSA and DMA, will simplify the applicable rules and increase legal certainty for businesses, making the EU more competitive and commercially attractive. However, the Commission's proposal to repeal the entire P2B Regulation, with only limited and time-gated exceptions, will lead to loopholes and weaknesses in the legal protections, that are disproportionate to the marginal reduction in administrative burdens that would be achieved. While simplification efforts are supported, they should not come at the expense of the essential safeguards for European SMEs. Such safeguards include transparency regarding general terms and conditions, predictability in the event of changes, insight into rankings and clear procedures in the event

Presidency first compromise text	Drafting suggestions and Comments
	of restriction or suspension. Their importance is reflected in the growing awareness of P2B rights and the increasing number of complaints concerning non-compliant platforms. The P2B Regulation contributes to the proper functioning of the single market by harmonising rules that afford transparency, fairness and effective redress tools to business users of platforms. In this regard, it has a specific approach and constitutes a first step toward establishing a comprehensive EU legal framework for online intermediaries. The DMA and DSA have different targets and scopes. They do not provide the same substantive obligations, nor do they offer the subsidiarity and proximity afforded by the P2B Regulation. Therefore, they cannot offer the same level of protection in such situations. Simplification efforts should lead to a genuine reduction in regulatory burden. ITALY believes that targeted adjustments to remove clear overlaps with the DSA and DMA would streamline the regulatory framework without dismantling essential protections. The limited administrative burden associated with the remaining P2B provisions, would be proportionate in light of the legal certainty and protection they afford SMEs. Therefore, WE propose to maintain certain essential P2B provisions on a permanent basis, while repealing the rest. This partial repeal reflects a more targeted and proportionate approach to reduce complexity and administrative burdens within the P2B Regulation while preserving the necessary protection this legislation offers for businesses, in particular SMEs. NL (Drafting suggestions): 59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU)

Presidency first compromise text	Drafting suggestions and Comments
	2022/2065 and Regulation (EU) 2022/1925 provide a ~~comprehensive~~ regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that **some** objectives and material provisions of the Platform-to-Business Regulation are ~~largely~~ covered by the Digital Services Act and the Digital Markets Act, Regulation (EU) ~~2019/1050~~**2019/1150** should be **partially** repealed. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty **and for purposes of keeping the necessary level of protection for business users**, ~~selected definitions in~~ **Articles 2, points (1) to (10) and (13), 3, 4, 5, 7, 10, 11, 15 and 19 should remain in application as they contain obligations that are not fully covered by Regulations (EU) 2022/2065 and (EU) 2022/1925.** NL (Comments): The Netherlands acknowledges and supports the Commission's efforts to reduce administrative burdens by avoiding potential overlaps between the P2B Regulation and other EU legislation. Addressing those parts of the P2B Regulation that clearly overlap with other EU legislation, primarily the DSA and DMA, will simplify the applicable rules and increase legal certainty for businesses, making the EU more competitive and commercially attractive. However, the Commission's proposal to repeal the entire P2B Regulation, with only limited and time-gated exceptions, will lead to loopholes and weaknesses in the legal protections, that are disproportionate to the marginal reduction in administrative burdens that would be achieved.

Presidency first compromise text	Drafting suggestions and Comments
	While simplification efforts are supported, they should not come at the expense of the essential safeguards for European SMEs. Such safeguards include transparency regarding general terms and conditions, predictability in the event of changes, insight into rankings and clear procedures in the event of restriction or suspension. Their importance is reflected in the growing awareness of P2B rights and the increasing number of complaints filed with the Dutch competition authority concerning non-compliant platforms. The P2B Regulation contributes to the proper functioning of the single market by harmonising rules that afford transparency, fairness and effective redress tools to business users of platforms. In this regard, it has a specific approach and constitutes a first step toward establishing a comprehensive EU legal framework for online intermediaries. The DMA and DSA have different targets and scopes. They do not provide the same substantive obligations, nor do they offer the subsidiarity and proximity afforded by the P2B Regulation. Therefore, they cannot offer the same level of protection in such situations. Simplification efforts should lead to a genuine reduction in regulatory burden. We believe that targeted adjustments to remove clear overlaps with the DSA and DMA would streamline the regulatory framework without dismantling essential protections. The limited administrative burden associated with the remaining P2B provisions, would be proportionate in light of the legal certainty and protection they afford SMEs. Therefore, we propose to maintain certain essential P2B provisions on a permanent basis, while repealing the rest. This partial repeal reflects a more targeted and proportionate approach to reduce complexity and administrative burdens within the P2B Regulation while preserving the necessary protection this legislation offers for businesses, in particular SMEs.

Presidency first compromise text	Drafting suggestions and Comments
(61) The amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 are based on Article 16 TFEU. The amendments to Directive 2002/58/EC are based on Article 16 TFEU and Article 114 TFEU. All other amendments are based on Article 114 TFEU.	
Article 3 **Amendments to Regulation (EU) 2016/679 (GDPR)**	
Regulation (EU) 2016/679 is amended as follows:	
	CZ (Drafting suggestions): **2. Article 2(4) is replaced by the following:** **'This Regulation shall be without prejudice to the application of Regulation 2022/2065, in particular the providers of intermediary services shall not be considered controllers when acting within the rules and conditions for limitation of their liability in Articles 4 to 8 of that Regulation.'** CZ (Comments): CZ: CZ believes that it is necessary to clarify the relation between DSA and GDPR regulation, because obligations to which the controller is subject would effectively void most of the limitations of the requirements that are afforded by DSA to providers of intermediary services.
1. Article 4 is amended as follows:	
~~(a) in point 1, the following sentences are added:~~	FI (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	Finland can support the Presidency compromise proposal to remove the amendments to the definition for personal data. Finland had concerns that the Commission's proposal would have gone beyond the CJEU case law and could have weakened the current level of data protection. LU (Comments): • **The definition of "personal data"** - Article 4 (a) in the CP read together with preamble (27a) The definition of personal data in the GDPR should remain unchanged. The CJEU's case law, that is legally binding, ensures that the notion of "personal data" remains both legally robust and adaptable. Introducing legislative modifications by summarizing a single CJUE's judgment would further complicate the Court's task by creating additional layers of interpretation, potentially generating uncertainty rather than resolving it. Instead of modifying the definition, we fully support mandating the EDPB to integrate the Court's guidance provided in Case C-413/23 P into forthcoming guidelines. We therefore support the proposed recital 27a as consequence.
~~'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'~~	CZ (Comments): CZ: CZ is open to more precise wording on identifiability of data subject, including through limited expansion of the definition in line with recital 26 GDPR, protecting legal certainty as much as possible. DK (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	As mentioned previously, DK considers it important to define the concept of relative anonymisation in order to ensure a greater degree of uniformity in enforcement Furthermore, DK notes the importance of this definition aligning with CJEU case law as pertaining to the C-413/23 P EDPS v SRB case. FI (Comments): Finland can support the Presidency compromise proposal to remove the amendments to the definition for personal data. Finland had concerns that the Commission's proposal would have gone beyond the CJEU case law and could have weakened the current level of data protection. IT (Drafting suggestions): "'Personal data' means any information relating to an identified or identifiable natural person **from the perspective of the specific controller or processor concerned**, taking into account the means reasonably likely to be used by that controller or processor for identification. A natural person shall be deemed identifiable only where identification can be achieved **by reasonable efforts in terms of cost, time, available technology and legal permissibility** by that controller or processor. Information shall not constitute personal data for a controller where identification would require disproportionate effort or access to data not lawfully available to that controller. Identification should be assessed **ex ante and in concreto**, considering the actual technical, organisational and legal capabilities of the controller."
(b) the following points are added:	

Presidency first compromise text	Drafting suggestions and Comments
'(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;	
(33) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;	
(34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;	
(35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;	NL (Comments): NL refers to its study reservation about the exemption for media service providers (Article 88b(3).
(36) 'media service provider' means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;'	NL (Comments): NL refers to its study reservation about the exemption for media service providers (Article 88b(3).
(37) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.'	
~~(38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'~~	CZ (Drafting suggestions): **(38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to**

Presidency first compromise text	Drafting suggestions and Comments
	ethical standards, including scientific methods, in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.' CZ (Comments): CZ: CZ does not agree with deletion of the definition of scientific data. EU should use this simplification instrument to ensure that its researchers are not subject to administrative burdens that prevent them to remain competitive on the world stage. However, scientific research is foremostly defined by using scientific methods, which should be explicitly mentioned. FI (Drafting suggestions): (38) "scientific research" means any research **for a scientific purpose carried out in accordance with the established ethical standards and the methodology applicable in the sector concerned by the research** which **may** ~~can~~ also support innovation, such as technological development and demonstration. **These actions shall be conducted in an autonomous and independent manner and lead to verifiable and transparent results**. These actions shall **also** contribute to existing scientific knowledge or apply existing **scientific** knowledge in novel ways~~,~~ **and** be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing ~~and adhere to ethical standards in the relevant research area~~. **[~~This does not exclude that the scientific research may also aim to further a commercial interest~~.]**' FI (Comments): Finland can show flexibility and continue discussions on the definition for scientific research.

Presidency first compromise text	Drafting suggestions and Comments
	At the same time, Finland underlines that Finland cannot support the original Commission proposal. Finland considers that the definition for 'scientific research' should be amended and clarified in order to ensure that the proposed definition is based on commonly accepted characteristics for the concept of scientific research. It is vital to add into the definition that 'scientific research' comprises any research that 1) has a scientific purpose and 2) complies with ethical standards and appropriate sector-specific methodology. Finland considers that these elements are mentioned in the recitals and should be transferred to the Article. Finland underlines that the EDPB-EDPS Joint Opinion proposes similar drafting suggestions. The EDPB-EDPS for instance propose adding that scientific research shall be conducted in an autonomous and independent manner and lead to verifiable and transparent results (see para 29, i). Finland considers that the last sentence in brackets may be transferred to the recitals (see also EDPB-EDPS Joint Opinion para 29, ii), but remains flexible if the Finnish drafting suggestions are taken into account in the posible definition. See **drafting suggestion striken, bolded and underlined**. Finland considers that the proposed definition for 'scientific research' could potentially lead to circumventing the obligations laid down in the GDPR if the research does not adhere to ethical and methodological standards and could be carried out mainly or purely for commercial interest. If, however, the new definition is removed, Finland considers that all of the accompanying recital text should be similarly removed (see comments concerning the recitals above). IT

Presidency first compromise text	Drafting suggestions and Comments
	(Drafting suggestions): Restore the definition LU (Comments): • **The definition of "scientific research" -** Article 4 (38) in the CP Luxembourg fully supports the objective of fostering research activities within the European Union, particularly in the field of innovative technologies. **Whether the proposed new definition is capable of effectively achieving this objective, however, remains under examination at national level**. it is moreover important to ensure full consistency between any proposed definition and recital 159 of the GDPR, which already provides interpretative guidance regarding the notion of scientific research. This will avoid creating discrepancies or parallel interpretations that could undermine the coherence of the existing framework.
2. Article 5 (1)(b) is replaced by the following:	
'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, **subject to the application of appropriate safeguards** in accordance with Article 89(1), be considered to be compatible with the initial ~~purposes, independent of the conditions of Article 6(4) of this Regulation,~~**purpose** ('purpose limitation');'	CZ (Drafting suggestions): 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, **subject to the application of appropriate safeguards** in accordance with Article 89(1), be considered to be compatible with the initial **purposes, independent of the conditions of Article 6(4) of this Regulation, ~~purpose~~** ('purpose limitation');' CZ

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): CZ believes that simplification is necessary and has been in fact already intended by GDPR, which is evident from its recital 50. As a matter of compromise, CZ can accept explicit reference to "appropriate safeguards". FI (Drafting suggestions): collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, **subject to the application of appropriate safeguards** in accordance with Article 89(1), be considered to be compatible with the initial purposes**, independent of the conditions of Article 6(4) of this Regulation,** ('purpose limitation'); FI (Comments): Finland can support adding the reference to appropriate safeguards in Article 5(1)(b) GDPR. However, Finland remains cautious to delete the following wording "~~purposes, independent of the conditions of Article 6(4) of this Regulation,~~" and proposes to keep the COM wording. See **drafting suggestion underlined and bolded**. See comments also in recital 29. IT (Drafting suggestions): Add final sentence to article 5(1)b: "Further processing of personal data for scientific research or technological development purposes also unrelated to the initial research shall be presumed compatible with the initial purpose and shall not require a new legal basis or renewed consent from the data subject."

Presidency first compromise text	Drafting suggestions and Comments
	LU (Comments): • **Principles relating to processing of personal data –** Article 5 (1) (b) in the CP We can support the deletion of the reference to Art. 6(4) and the addition of safeguards. To facilitate the possibility of further processing, we suggest to partially include recital 50 of the GDPR in Article 5(1)(b). To be more precise, we suggest specifying that in case of compatible further processing, no legal basis - separate from that which allowed the collection of the personal data- is required.
	IT (Drafting suggestions): Amendment to Article 6(1) – new sub-paragraph "When assessing the lawfulness of processing pursuant to paragraph 1, competent authorities and courts shall ensure an equitable balancing between the protection of personal data and other fundamental rights and freedoms recognised by Union law, including the freedom to conduct a business."
3. Article 9 is amended as follows:	
	BE (Drafting suggestions): **Paragraph 1 is amended as follows:** **Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health**

Presidency first compromise text	Drafting suggestions and Comments
	or data concerning a natural person's sex life or sexual orientation shall be prohibited. **For the purposes of this Regulation, biometric data used solely for the purpose of verifying the claimed identity of a data subject through a one-to-one comparison shall not in itself be considered biometric identification.**
(a) in paragraph 2, the following points are added:	
	IT (Drafting suggestions): *Replacement of Article 9(2)(j)* "(j) processing is necessary for scientific research or technological development purposes, including in the fields of medicine, biotechnology, neurotechnology, biomedical engineering, bionics, robotics, brain-computer interface systems, organ bioprinting and related health-innovation activities, subject to appropriate technical and organisational safeguards ensuring data minimisation, security and functional separation. Processing of personal data that is necessary for scientific research or technological development pursued in the public interest, including health-related research and innovation, shall be deemed lawful without requiring the consent of the data subject, provided that appropriate safeguards pursuant to Article 89 are implemented"
'(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5.	FI (Drafting suggestions): '(k) **incidental and residual** processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5. FI

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): Finland proposes to clarify that the proposed derogation applies to only incidental and residual processing of special categories of data, similarly as the EDPB-EDPS Joint Opinion (para 48, 49). See **drafting suggestion bolded and underlined.** IT (Comments): The scope of Article 9(2)k should be clarified and aligned to the correspondent recital 33 which only refers to the **residual** processing of special categories of data in the context of the development of AI systems or models. In line with what highlighted by the EDPB/EDPS in the Opinion on Digital Omnibus, Article 9(2)(k) GDPR should not be understood as covering the processing of special categories of personal data collected through prompts, for training purposes, during the deployment of the AI system or model. NL (Drafting suggestions): ~~'(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5~~. NL (Comments): - The NL is concerned that this proposed novel exception to the prohibition on the processing of special categories of data may significantly reduce the protection of special categories of personal data in the context of AI development and operation.

Presidency first compromise text	Drafting suggestions and Comments
	- Operators of AI systems would be allowed to process special categories of personal data if its removal would cause "disproportionate effort". This reverses the protective logic of data protection law and risks creating a perverse incentive: the more data is processed, the easier it becomes to justify the processing of special categories of personal data. - Personal data which are processed via an AI system would be treated more favourable than any "normal" (lower risk) processing operation, which would deviate from the technology-neutral nature of the GDPR. This risks creating situations wherein controllers might unnecessarily use AI simply to make use of this exception.
(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the **one-to-one** verification is under the sole control **and possession** of the data subject~~.~~ **and in so far as it is authorised by Union or Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject'**	BE (Drafting suggestions): (l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the **one-to-one** verification is under the sole control **and possession** of the data subject~~.~~ **~~and in so far as it is authorised by Union or Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject'~~**, **including where such verification is required in order to comply with obligations under Union law relating to electronic identification and trust services (eIDAS), subject to appropriate safeguards laid down in Union or Member State law to protect the fundamental rights and interests of the data subject.** BE (Comments): **Relationship with the eIDAS framework** The relationship between the proposed exemption in Article 9 and identity-verification processes carried out under the eIDAS framework must be clarified, in particular Commission Implementing Regulation (EU)

Presidency first compromise text	Drafting suggestions and Comments
	2015/1502, which in practice may rely on biometric verification (e.g. remote onboarding). Such clarification could help ensure legal certainty for organisations required to comply with both EU electronic identification rules and the GDPR. **Identification vs verification** The distinction between biometric identification (one-to-many comparison) and biometric verification (one-to-one comparison used to confirm a claimed identity) must be clarified, as several authentication solutions, including digital wallet applications, rely on the latter where the biometric data remain under the control of the user. Clarification could help avoid divergent interpretations across Member States. CZ (Drafting suggestions): (l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the **one-to-one** verification is under the sole control **and possession** of the data subject~~.~~ **~~and in so far as it is authorised by Union or Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject'~~** CZ (Comments): CZ: CZ is against the necessity to adopt EU or domestic legislation for the mere verification that is practically under sole control of data subject. Appropriate safeguard is already provided by the provision itself. This would essentially force Member States to design unnecessary legislative burdens that would only prevent free flow of European verification solutions. If a Member State identifies grave need to require such safeguards, relevant legislation can already be adopted under Art. 9(4) GDPR.

Presidency first compromise text	Drafting suggestions and Comments
	DK (Comments): DK prefers the Commission's proposal to avoid the risk of fragmentation. FI (Drafting suggestions): l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the **one-to-one** verification is under the sole control **and possession** of the data subject~~. and in so far as it is authorised by Union or Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject'.~~ FI (Comments): Finland can support the proposed clarifications to the Article and to the recitals. However, Finland is not convinced whether this derogation should rely on Member State/Union law. See **drafting suggestion striken, bolded and underlined.** See also comments and drafting suggestions in the accompanying recitals. LU (Comments): • **Biometric Verification –** Article 9 (l) in the CP We support the overall objective of this provision. Regarding the modifications made by the PRES, we are not favorable to foresee an additional authorisation by national law since this would go against the objective of simplification by leading to new fragmentation of legal regimes.

Presidency first compromise text	Drafting suggestions and Comments
	NL (Drafting suggestions): (l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the one-to-one verification is under the sole control and possession of the data subject~~.~~ ~~and in so far as it is authorised by Union or Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject~~ NL (Comments): According to NL, it is not necessary to require authorisation by Union or Member State law providing for appropriate safeguards, because Article 9(2)(l) and recital 34 contain sufficient safeguards. This must be seen in the light of the fact that the current Article 9(1) does not prohibit the processing of biometric data for *verification* purposes, but prohibits the processing of "biometric data for the purpose of uniquely *identifying* a natural person". Identification is a one-to-many matching process (who are you?), while verification is a one-to-one matching process (are you who you say you are?). If appropriate, Member States can regulate additional safeguards on the basis of the current Article 9(4).
(b) the following paragraph is added:	
'5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller	FI (Drafting suggestions): 5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies

Presidency first compromise text	Drafting suggestions and Comments
shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.'	special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data **is not possible or** requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being **processed for other purposes, from being** used to produce outputs, from being disclosed or otherwise made available to third parties.' FI (Comments): Clarifications based on EDPB-EDPS Joint Opinion (paras 48-52). See **drafting suggestions bolded and underlined**. See also comments and drafting suggestions in the accompanying recitals. IT (Drafting suggestions): If removal of those data **is impossible or** requires disproportionate effort, **based on a properly documented effort, considering the state-of-the-art technology and the impact on data subjects,** the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties. IT (Comments): The suggestion aims at better substantiating the cases of impossibility or disproportionate effort of the removal NL (Drafting suggestions): ~~'5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the~~

Presidency first compromise text	Drafting suggestions and Comments
	~~collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.'~~ NL (Comments): See art. 9(2)(k).
	BE (Drafting suggestions): **6. Processing of biometric data pursuant to point (l) shall be subject to appropriate technical and organisational measures to ensure that such processing is limited to identity verification and does not involve biometric identification through comparison against a database intended to determine the identity of a natural person.**
4. In Article 12, paragraph 5 is replaced by the following:	
'5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character ~~or also, for~~**and, in the case of** requests under Article 15**, where an abusive intention on the part of** ~~because~~ the data subject ~~abuses the rights conferred by this regulation for purposes other than the protection of their data~~**submitting those requests can be demonstrated**, the controller may either:	FI (Comments): Finland can support the proposed amendments and considers it vital that the Commission's original text "abuses the rights conferred by this regulation for purposes other than the protection of their data" is removed as it would weaken the current level of data protection. LU (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	• **Access requests -** Article 12, paragraph 5 in the CP Luxembourg would like to express its overall support for this provision. We are however not sure what the notion of "abusive intention" entails. Unlike that of "abuse of rights" which is a commonly referenced notion in European law, this notion seems novel. It is important to make sure that the desired situations are covered by this exception. We support the inclusion of further guidance with regards to this notion in the recitals of the GDPR. NL (Drafting suggestions): '5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character ~~and,~~ ~~in the case of requests under Article 15,~~ **including requests** where an abusive intention on the part of the data subject submitting those requests can be demonstrated, the controller may either: NL (Comments): NL considers that if Article 12(5) would be extended with the possibility to refuse a data access request because of an abusive intention, this possibility should also apply to other data subject rights to avoid the impression that an abusive intention is only relevant in case of data access requests. As Austria rightly noted in its amendment (WK 1701/2026 INIT, page 85/86) the addition to Article 12(5) should apply to all data subject rights in order to maintain consistency, because requests for rectification or erasure could be misused in a similar way as requests for access.

Presidency first compromise text	Drafting suggestions and Comments
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or	
(b) refuse to act on the request.	
The controller shall bear the burden of demonstrating that the request is manifestly unfounded or ~~that there are reasonable grounds to believe that it is~~ excessive**, or that the request is submitted with an abusive intention**.'	FI (Comments): Finland can support the proposed amendment. See comments above.
5. In Article 13, paragraph 4 is replaced by the following:	
'4. Paragraphs 1, 2 and 3 shall not apply where **and insofar as the data subject has the information and where** the personal data ~~have been~~**are** collected in the context of a ~~clear and~~**direct, limited and clearly** circumscribed relationship between data subjects and a controller exercising an activity that is not ~~data-intensive~~**likely to result in a high risk to the rights and freedoms of data subjects nor involve the processing of large amounts of personal data, special categories of personal data or complex processing operations** and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1~~, unless~~**.** **The first subparagraph shall not apply where** the controller **intends to process the data collected from the data subject for other purposes,** transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.'	FI (Drafting suggestions): 4. Paragraphs 1, 2 and 3 shall not apply where **and insofar as the data subject has the information and where** the personal data ~~have been~~**are** collected in the context of a ~~clear and~~**direct, limited and clearly** circumscribed relationship between data subjects and a controller exercising an activity that is not ~~data-intensive~~**likely to result in a high risk to the rights and freedoms of data subjects nor involve the processing of large amounts of personal data, special categories of personal data, personal data relating to criminal convictions and offences referred to in Article 10 or complex processing operations** and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1~~, unless~~**.** **The first subparagraph shall not apply where** the controller **intends to process the data collected from the data subject for other purposes,** transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a

Presidency first compromise text	Drafting suggestions and Comments
	high risk to the rights and freedoms of data subjects within the meaning of Article 35.' FI (Comments): Finland thanks the Presidency for considering the Finnish drafting suggestions. Finland considers it vital to replace the wording "data-intensive" and considers that a reference to high-risk processing and processing special categories of personal data, etc. is a good alternative. In addition, Finland proposes the Presidency to refer to personal data referred in Article 10 GDPR as well. Finland has also concerns whether for instance "complex operations" is sufficiently clear. In this regard Finland welcomes the Presidency to evaluate whether "complex operations" could be replaced with a reference to Article 37(1)(b) GDPR which refers to processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. See **drafting suggestion bolded and underlined** LU (Drafting suggestions): Paragraphs 1 **and**, 2 ~~and 3~~ shall not apply ~~where and insofar as the data subject has the information~~ where the personal data are collected in the context of a direct~~limited~~ and clearly circumscribed relationship between **the** data subjects and **the** controller ~~exercising an activity that is not likely to result in a high risk to the rights and freedoms of data subjects~~ nor involve**s** the processing of large amounts of personal data, special categories of personal data or complex processing operations

Presidency first compromise text	Drafting suggestions and Comments
	and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1**, unless** ~~The first subparagraph shall not apply where~~, transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35." LU (Comments): • **Information requirements** – Article 13, paragraphs 4 and 5 in the CP We support the overall objective pursued by the modifications, read together with recital 36. It is moreover important that the latter recital provides concrete examples of the nature of the exemption, such as the relationship between a craftsman and their clients, where the scope of processing is limited to the minimum data necessary to perform a service. We suggest leaving out the word "limited" - the scope of which is not clear - and keeping a "direct and clear circumscribed relationship between the data subject and the data controller". Furthermore, if the phrase according to which "*insofar as the data subject has the information*", added in the last PRES compromise text, has the same scope as the phrase "*and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1*", we propose to only keep the second one - that is more detailed. We also preferred the previous wording where the provision had only one paragraph ("unless") and not two subparagraphs. This because the first subparagraph already starts with a derogation ("shall not apply"). The second subparagraph repeats a derogation - making it difficult to understand because it is a double negation.

Presidency first compromise text	Drafting suggestions and Comments
	Lastly, there is a problem between subparagraph 1 and 2 because the first excludes the application of Article 13(3) whereas the second *subparagraph* includes it again. The same applies for the reference to the high risk to the rights and freedoms of the data subject. Additionally, we would like to highlight that the derogation sought by the new paragraph 4 will be considerably limited by including an information obligation when special categories of personal data are processed. We understand the intention and rationale behind the introduction. However, we would like to bring to the attention of delegations that a lot of associations as well as sport clubs process this kind of data to organize membership or events. The objective of simplification and clarification of the GDPR would be significantly weakened for these kinds of stakeholders. NL (Drafting suggestions): 4. Paragraphs 1, 2 and 3 shall not apply**:** **(a)** where and insofar as the data subject has the information **or** ~~and~~ **(b)** where **there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 and** the personal data are collected in the context of a direct, limited and clearly circumscribed relationship between data subjects and a controller exercising an activity that is not likely to result in a high risk to the rights and freedoms of data subjects nor involve the processing of large amounts of personal data, special categories of personal data or complex processing operations ~~and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1~~. ~~The first~~ **S**~~s~~ubparagraph **b** shall not apply where the controller intends to process the data collected from the data subject for other purposes, transmits

Presidency first compromise text	Drafting suggestions and Comments
	the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.' NL (Comments): The existing exception to the information obligation, laid down in the current Article 13(4), appears to be erroneously deleted. This results in a complication rather than a simplification. Therefore, the NL proposes to split the proposed Article 13(4) in two subparagraphs and to keep the current Article 13(4) in subparagraph 4a. The new exception should be moved to subparagraph 4b. To clarify the relation between the two subparagraphs, the clause "*there are reasonable grounds to assume that the data subject already has the information…*" should be brought to the front, to mark the contrast with subparagraph 4a ("*…has the information*").
6. In Article 13, paragraph 5 is added:	
'5. When the **further** processing takes place for scientific research purposes **by the same controller and where and insofar as** ~~and~~ the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort ~~subject to the conditions and safeguards referred to in Article 89(1)~~ or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that **further** processing**, subject to the conditions and safeguards referred to in Article 89(1)**, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.'	DK (Drafting suggestions): '5. When the **further** processing takes place for scientific research purposes ~~**by the same controller and where and insofar as**~~ and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort ~~subject to the conditions and safeguards referred to in Article 89(1)~~ or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that **further** processing**, subject to the conditions and safeguards referred to in Article 89(1)**, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take

Presidency first compromise text	Drafting suggestions and Comments
	appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.' DK (Comments): As previously mentioned, DK does not support the proposed limitation of when the exemption from the obligation to provide information applies in relation to scientific research. As we see it, it should also apply to disclosure as it was originally proposed.
~~7. In Article 22, paragraphs 1 and 2 are replaced by the following:~~	CZ (Drafting suggestions): **7. In Article 22, paragraph 2 point (a) is amended as follows:** FI (Drafting suggestions): **7. In Article 22, paragraph 2, point (a) is replaced by the following:** FI (Comments): Finland considers that this Digiomnibus proposal could clarify the application of Article 22(2)(a) of the GDPR. See also EDPB-EDPS Joint Opinion (paras 68-69). See **drafting suggestion bolded and underlined.** LU (Comments): • **Automated Decision Making** – Article 22 in the CP We consider it useful to simplify this provision's drafting which is currently rather complex. Article 22 of the GDPR has long been regarded as offering

Presidency first compromise text	Drafting suggestions and Comments
	limited legal clarity and is frequently perceived as difficult to understand in practice. This is especially relevant In light of the latest case law of the CJEU (case C-634/21 SCHUFA Holding (Scoring)) and the entry into force of the AI Act. Moreover, in its current wording, the concrete legal consequences of the explicit reference of a 'right' not to be subject to an automated decision remain uncertain, a point clearly reflected in the ongoing debate surrounding this provision. We will however, at this stage, not insist on the reinsertion of the Commission's proposal.
~~'1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:~~	
~~(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;~~	CZ (Drafting suggestions): **'(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;'** CZ (Comments): CZ agrees with the Presidency that the right not to be subject to automated decisions and the fundamental structure of Article 22 should be maintained, but in order to simplify conditions for development of European digital economy, finds it advisable and beneficial to clearly enable automated decision-making online in the context of preparation and conclusion of contracts.

Presidency first compromise text	Drafting suggestions and Comments
	FI (Drafting suggestions): **(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;** FI (Comments): Finland considers that this Digiomnibus proposal could clarify the application of Article 22(2)(a) of the GDPR. See also EDPB-EDPS Joint Opinion (paras 68-69). See **drafting suggestion bolded and underlined.**
~~(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or~~	
~~(c) is based on the data subject's explicit consent.~~'	
8. Article 33 is amended as follows:	
(a) paragraph 1 is replaced by the following:	
'1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~96~~**72** hours after having become aware of it, notify the personal data breach **[**via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555**]** to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.'	BE (Comments): Belgium prefers the 96-hour deadline, as proposed by the Commission, supported by the EDPB, to allow better quality over speed in assessments. If 72 hours is retained, the "where feasible" qualification must remain, and the SEP provision should be retained with confidentiality guarantees for data transmitted. Regardless of the deadline chosen, the use of a Single Entry Point via NIS2 is instrumental to reduce cross-regulatory duplication.

Presidency first compromise text	Drafting suggestions and Comments
	CZ (Drafting suggestions): '1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~9672~~ **96** hours after having become aware of it, notify the personal data breach **[**via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555**]** to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. **However, where such a personal data breach does not concern cross-border processing, the controller may notify a personal data breach directly to the competent supervisory authority.** Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.' CZ (Comments): CZ: In light of the flexible position of Joint Opinion by EPDB and EDPS, CZ proposes to alleviate the obligations of controllers (in particular smaller ones with less IT and legal capacities) and provide longer reporting deadline of 96 hours. This would decrease cost of regulation to smaller controllers in particular. CZ suggest simplifying the situation for purely national - and likely small - processing (excluding cases under Art. 4 point 23 GDPR), but in light of ongoing discussions on SEP is willing to await further developments. FI (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
	1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~96~~**72** hours after having become aware of it, notify the personal data breach **[**via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555**]** to the supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within **72** ~~96~~ hours, it shall be accompanied by reasons for the delay. FI (Comments): Finland supports to remain the current deadline of 72 hours. Finland has only a technical comment: the deadline should be amended also in the last sentence. See **drafting suggestion striken, underlined and bolded.** LU (Comments): We understand that the rationale behind the extension of the deadline from 72 to 96 hours in the Commission's proposal hours would help data controllers gather more information on the data breaches which would, in turn, also help data protection authorities. We therefore express our support for the initial proposal extending the deadline for such notifications from 72 to 96 hours. NL (Drafting suggestions): 1. In the case of a personal data breach that is likely to result in a**n impactful** ~~high~~ risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach [~~via the single-entry point established pursuant to Article 23a of Directive (EU)~~

Presidency first compromise text	Drafting suggestions and Comments
	~~2022/2555~~] to the supervisory authority competent in accordance with Article 55 and Article 56 of this Regulation. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.' NL (Comments): NL supports the aim to reduce disproportionate numbers of data breach notifications to data protection authorities. However, the Dutch Data Protection Authority observes that controllers often underestimate the risk of data breaches to data subjects. In such cases, DPAs could currently oblige controllers to notify a data breach to data subjects as well (Article 34(4) GDPR). By making the threshold for notification to the DPA the same as for notification to data subjects, DPAs will lose this "corrective" function, which could lead to data subjects staying unaware of data breaches. NL intends to maintain this corrective function, but also supports the aim to reduce disproportionate numbers of data breach notifications to DPAs. Therefore, NL proposes to find a compromise between the current threshold in Article 33 ("a risk") and the proposed threshold in the Commission proposal ("high risk"). A compromise could for example be "impactful risk" or alternatively, "relevant risk" or "increased risk". The formulation could further be explored. Regarding the single-entry point, see below.
(b) the following paragraph is added:	
'1a. Until the establishment of the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56 **of this Regulation**.'	NL (Drafting suggestions): '~~1a. Until the establishment of the single-entry point pursuant to Article 23a of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56 of this Regulation.'~~

Presidency first compromise text	Drafting suggestions and Comments
	NL (Comments): A single-entry point at EU-level should not overlap with existing national reporting structures. Moreover, notifications may include sensitive information related to the essential or national security interests of Member States. Therefore, Member States should at all times remain the direct and sole recipient of notifications and the processing of notifications (including personal data breaches) should remain the sole responsibility of the Member States.
(c) the following paragraphs are added:	
'6. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as ~~for~~ a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person **and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists**~~. The proposals~~ shall be ~~submitted to the Commission~~**available** within [OP date = nine months of the entry into application of this Regulation]. ~~The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).~~	BE (Comments): Belgium supports the Presidency compromise giving the EDPB direct authority to establish and publish the template and high-risk list, without the Commission's implementing act mechanism FI (Comments): Finland can support the changes and in general considers that the EDPB should establish and publish these templates and lists. However, Finland also underlines that it should be clear what is meant by high-risk processing. NL (Drafting suggestions): '6. The Board shall establish and make public a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as a list of the circumstances in which a personal data breach is likely to result in a**n impactful** ~~high~~ risk to the rights

Presidency first compromise text	Drafting suggestions and Comments
	and freedoms of a natural person and a list of the circumstances in which it is not likely to result in such a ~~high~~ risk. The template and lists shall be available within [OP date = nine months of the entry into application of this Regulation]. NL (Comments): See paragraph 1.
7. The template and ~~the list~~**lists** referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. ~~The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6.'~~	FI (Comments): Finland can support the proposed changes and in general considers that the EDPB should establish and publish these templates and lists.
	NL (Drafting suggestions): 7a. In Article 34, the following paragraph is added: **5. The Board shall establish and make public a common template for notifying a personal data breach to data subjects as well as a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person and a list of the circumstances in which it is not likely to result in such a risk. Article 33(6), second sentence, and 33(7) apply accordingly.** NL (Comments): This amendment mirrors Article 33, paragraph 6 and 7, for the notification of data breaches to data subjects. This is necessary because of the NL proposal for different risk thresholds in Articles 33 and 34. Furthermore, a common template could also be helpful for notifications to data subjects.

Presidency first compromise text	Drafting suggestions and Comments
9. Article 35 is amended as follows:	
(a) paragraphs 4, 5 and 6 are replaced by the following:	
'4. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.	BE (Comments): Belgium supports the Presidency's approach of empowering the EDPB to establish and make public DPIA lists directly, removing the Commission implementing act layer. FI (Comments): Finland can support the changes and in general considers that the EDPB should establish and publish these templates and lists.
5. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** a list of the kind of processing operations for which no data protection impact assessment is required.	FI (Comments): Finland can support the changes and in general considers that the EDPB should establish and publish these templates and lists.
6. The Board shall ~~prepare and transmit to the Commission a proposal for~~**establish and make public** a common template and a common methodology for conducting data protection impact assessments.'	FI (Comments): Finland can support the changes and in general considers that the EDPB should establish and publish these templates and lists.
(b) the following ~~paragraphs are~~**paragraph is** inserted:	NL (Drafting suggestions): (b) the following **paragraphs are** ~~paragraph is~~ inserted:

Presidency first compromise text	Drafting suggestions and Comments
~~'6a. The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission within [OP date = 9 months of the entry into application of this Regulation]. The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).~~	FI (Comments): Finland can support the changes and in general considers that the EDPB should establish and publish these templates and lists. NL (Drafting suggestions): 6a. The ~~proposals for the~~ lists referred to in paragraphs 4 and 5 and ~~for~~ the template and methodology referred to in paragraph 6 shall be **published** ~~submitted to the Commission~~ within [OP date = 9 months of the entry into application of this Regulation]. ~~The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).~~ NL (Comments): This paragraph seems to be erroneously deleted.
~~6b. The lists and the template and methodology referred to in paragraph 6a shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a.~~	FI (Comments): Finland can support the changes and in general considers that the EDPB should establish and publish these templates and lists. NL (Drafting suggestions): 6b. The lists and the template and methodology referred to in paragraph 6a shall be reviewed at least every three years and updated where necessary. ~~The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the~~

Presidency first compromise text	Drafting suggestions and Comments
	~~proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a.~~ NL (Comments): This paragraph seems to be erroneously deleted.
6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the ~~Commission adopts the implementing act~~**Board establishes and makes public the lists** referred to in paragraph ~~6a~~**4 and 5**.'	FI (Comments): Finland can support the changes and in general considers that the EDPB should establish and publish these templates and lists.
	CZ (Drafting suggestions): **6d. The supervisory authority may establish and make public lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required, only where such lists are not in contravention of the lists referred to in paragraph 4 and 5. The supervisory authority shall communicate those lists to the Board.'** CZ (Comments): CZ supports EU-wide lists and is flexible as regards the competences of Commission or the Board. However, complementary national lists should be possible to address local, specific or emerging issues. These lists should be reported to Board to ensure compatibility with EU-wide lists.
10. ~~The following article is added:~~	CZ

Presidency first compromise text	Drafting suggestions and Comments
	(Drafting suggestions): **10. The following article is added**
	IT (Drafting suggestions): Replacement of article 36(1) "1. By way of derogation from this Article, where processing is carried out exclusively for scientific research or technological development purposes within the meaning of Article 89, the controller shall notify the competent supervisory authority prior to the commencement of processing. Such processing shall not be subject to prior consultation or authorisation by the supervisory authority." New Article 36(4) "4. The notification referred to in paragraph 1 shall contain a general description of the research purposes, categories of data processed, safeguards adopted and expected duration of processing. The supervisory authority may issue non-binding recommendations but shall not suspend or prohibit the processing unless manifest and serious risks to fundamental rights are demonstrated."
~~'Article 41a~~	CZ (Drafting suggestions): **Article 41a** CZ (Comments): CZ understands that implementing acts should not directly determine the notion of personal data. However, the ability to determine where pseudonymised data are no longer personal data for certain entities is - albeit indirect and relative - delimitation of the notion of personal data, which is a basic element of the GDPR. Therefore, CZ believes that this Article should, at

Presidency first compromise text	Drafting suggestions and Comments
	the very least, include the core requirements on the means and criteria, similar to core requirements on adequacy decisions. This binding stipulation of core requirements for any such implementing act should be done by introducing the reason for why the data lose the status of personal data in relation to specific entities in para (1) and by adapting point 2(b) to cover the basic factors contributing to risk of re-identification (according to recital 26 GDPR). Words "or reasonably foreseeable" are added to address risk-based determination of other than typical or intended recipients (including criminal actors where reasonably relevant).
	FI (Drafting suggestions): **Technical means and criteria for pseudonymisation** FI (Comments): Finland proposes a heading to Article 41a, if this Article is not removed.
~~(1) The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.~~	CZ (Drafting suggestions): **(1) The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities because those entities are not reasonably likely to identify the natural person.** FI (Drafting suggestions): **(1) The Commission may adopt implementing acts to specify technical means and criteria for pseudonymization.** FI (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	Finland can support to delete Article 41a, but remains flexible, as it is important to provide technical assistance to the controllers and processors. However, Finland cannot as such support the Commission's proposal and underlines that possible implementing acts should be limited to technical aspects. Finland has provided drafting suggestion earlier and respectfully repeats it.
~~(2) For the purpose of paragraph 1 the Commission shall:~~	CZ (Drafting suggestions): **(2) For the purpose of paragraph 1 the Commission shall:** FI (Drafting suggestions): **(2) For the purpose of paragraph 1 the Commission shall:**
~~(a) assess the state of the art of available techniques;~~	CZ (Drafting suggestions): **(a) assess the state of the art of available techniques;** FI (Drafting suggestions): **(a) assess available pseudonymisation techniques; and**
~~(b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.~~	CZ (Drafting suggestions): **(b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical or reasonably**

Presidency first compromise text	Drafting suggestions and Comments
	foreseeable recipients of data, based on costs, amount of time required, available technology, legal powers and restrictions and all relevant other objective factors. FI (Drafting suggestions): **(b) develop technical means and criteria for controllers and recipients to assess available pseudonymisation techniques.**
~~(3) The implementation of the means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.~~	CZ (Drafting suggestions): **(3) The implementation of the means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.** FI (Drafting suggestions): **(3) The implementation of the technical means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.**
~~(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.~~	CZ (Drafting suggestions): **(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.** FI (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
	(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.
~~(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).'~~	CZ (Drafting suggestions): **(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).'** **(6) The implementing acts shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments. The implementing act shall specify its territorial and sectoral application.'** CZ (Comments): CZ: CZ proposes to add further rules governing the implementing acts, similar to Article 45(3) GDPR. In particular, CZ proposes to establish firm deadline when the Commission must consider again all the relevant factors, in particular the developments as regards state of the art. FI (Drafting suggestions): **(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).**
	CZ

Presidency first compromise text	Drafting suggestions and Comments
	(Drafting suggestions): **10a. In Article 49(4), the following sub-paragraphs are added:** **This shall include cases where the transfer is necessary for the implementation, application or compliance with international or administrative agreements on mutual assistance or cooperation concluded by a Member State, including cases where personal data is exchange on a large scale and in a systematic manner, and where such agreements do not provide for appropriate safeguards within the meaning of Article 46. In such cases, Member States shall ensure that appropriate safeguards for the protection of data subjects are provided for under Union law or the law of the Member State, including personal data in transit as well as after such transaction has taken place.** **[Personal data shall not be transferred where the competent authority responsible for the transfer considers that the rights and freedoms of the data subject concerned override the public interest pursued by the transfer.]** **Transfers based on this Article shall be documented.** CZ (Comments): CZ: CZ strongly supports ES proposal Option 1, preferably without bracketed second new subparagraph, which is not usual in tax cooperation, could be difficult to implement and involves potentially large administrative burden. IT (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
	New Article 51a – Functional separation of Powers "1. Supervisory authorities shall be exclusively competent for administrative monitoring, investigative activities and the imposition of administrative corrective measures under this Regulation. 2. The protection and adjudication of subjective rights and obligations arising from this Regulation shall remain the exclusive competence of independent courts and tribunals of the Member States. 3. Decisions of supervisory authorities producing legal effects shall be subject to full judicial review."
11. In Article 57(1) is amended as follows:	CZ (Comments): CZ: CZ proposes to keep this deletion as the possibility under Art. 35(6d) would remain only option, not a task. NL (Drafting suggestions): 11. ~~In~~ Article 57~~(1)~~ is amended as follows:
	IT (Drafting suggestions): Amendment to Article 58(1) "1. Each supervisory authority shall have all of the following investigative powers **which shall not entail the determination of civil liability or the final determination of fundamental rights**." **2. Administrative enforcement procedures under this Regulation may involve punitive elements. Therefore, controllers and processors shall benefit from procedural guarantees equivalent to those recognised in the case-law of the Court of Justice and the European Court of Human Rights, including the privilege against self-incrimination.**

Presidency first compromise text	Drafting suggestions and Comments
	3. During investigations and proceedings conducted by supervisory authorities, controllers and processors shall have the right not to provide statements or information which would amount to an admission of an infringement liable to administrative, civil or criminal sanctions. **4. Prior to the adoption of any corrective measure or administrative fine, the controller or processor shall be granted:** **(a) access to the file;** **(b) the right to be heard;** **(c) adequate time and facilities to prepare a defence;** **(d) the right to legal representation.** **Evidence obtained in violation of these guarantees shall be inadmissible.** **5. Where investigative or corrective measures are liable, by their nature, severity or deterrent purpose, to be classified as criminal in substance within the meaning of the criteria established in the jurisprudence of the European Court of Human Rights (Engel and others v. Netherlands), supervisory authorities shall ensure compliance with the procedural safeguards applicable to criminal proceedings, including proportionality of inspections, prior judicial authorisation where appropriate, and respect for defence rights.** **The classification of administrative fines under this Regulation shall take into account their punitive and deterrent character."**
(a) point (k) is deleted;	NL (Drafting suggestions): (a) In paragraph 1, point (k) is deleted;
	NL (Drafting suggestions): (b) Paragraph 4 is replaced by the following: 4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, **including requests where an abusive intention on the part of the data subject submitting those requests can be**

Presidency first compromise text	Drafting suggestions and Comments
	demonstrated, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request **or that the request is submitted with an abusive intention**. NL (Comments): NL proposes to adapt Article 57(4) in line with Article 12(5) to maintain the existing consistency between these provisions. The EDPB and the EDPS also suggest this in §59 of their opinion on the Digital Opinion, to provide supervisory authorities with equivalent possibilities in relation to complaints.
12. In Article 64(1), point (a) is deleted.	CZ (Drafting suggestions): 12. In Article 64(1), point (a) is **amended as follows:** CZ (Comments): CZ: CZ proposes to change the power of EDPB to take into account possibility of supervisory authorities to adopt complementary compatible lists under Art. 35(6d).
	CZ (Drafting suggestions): **(a) aims to adopt a complementary list of the kind of processing operations pursuant to Article 35(6d);** NL (Drafting suggestions): 12a. In Article 70(1), point (g) is replaced with the following:

Presidency first compromise text	Drafting suggestions and Comments
	‘(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches, and determining the undue delay referred to in Article 33(1) and (2) and **34(1), and establish and publish the common template and lists referred to in Article 33(6) and 34(5)** for the particular circumstances in which a controller or a processor is required **or is not required** to notify the personal data breach;’ NL (Comments): These changes are necessary because of the changes which NL proposes to Articles 33 and 34(5). For reasons of simplification, NL also proposes to merge the proposed Article 70(1)(hc) with the existing Article 70(1)(g) and the deleted Article 70(1)(h), because all these provisions regard the notification of data breaches.
13. In Article 70(1), point (h) is deleted.	
14. In Article 70(1), the following points are inserted:	
‘(ha) ~~prepare and transmit to the Commission a proposal for~~**establish** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35.	
(hb) ~~prepare and transmit to the Commission a proposal for~~**establish** a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35.	
(hc) ~~prepare and transmit to the Commission a proposal for~~**establish** a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a	NL (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
personal data breach is likely to result in a high risk to the rights and freedoms of a natural person pursuant to Article 33 **and a list of the circumstances in which it is not likely to result in such a high risk**	~~(hc) prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person pursuant to Article 33'~~ NL (Comments): This provision has been incorporated into Article 70(1)(g), as proposed by NL.
hca issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph on pseudonymisation, clarifying circumstances whether a natural person is identifiable and means reasonably likely to be used to identify a natural person, and specifying means and criteria to determine whether data resulting from pseudonymisation may no longer constitute personal data for certain entities'	CZ (Drafting suggestions): **hca issue opinion on the draft implementing act to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities pursuant to Article 41a(4)'** CZ (Comments): CZ believes that an implementing act is much more preferable in terms of legal certainty and uniform application within EU, with at least the standard benefits for demonstrating compliance that are used Art. 24, 25, 28, 32 GDPR. It is a substantial factor of Digital Omnibus having an economic impact. Therefore, EDPB should be involved in preparation of implementing acts in a manner determined by Article 41a. FI (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
	hca issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph on pseudonymisation, <u>defined in Article 4, point (5),</u> clarifying circumstances <u>where personal data can no longer be attributed to a specific data subject without the use of additional information</u> ~~whether a natural person is identifiable and means reasonably likely to be used to identify a natural person, and specifying means and criteria to determine whether data resulting from pseudonymisation may no longer constitute personal data for certain entities~~' FI (Comments): Finland can support this new provision on guidelines concerning pseudonymisation but welcomes the Presidency to utilise the current definition for pseudonymisation in Article 4, point 5 GDPR. See **drafting suggestion bolded and underlined**. Article 4(5) GDPR: (5) 'pseudonymisation' *means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information*, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
	CZ (Drafting suggestions): **<u>14a. In Article 77 paragraph 3 is added:</u>** **<u>3. Member States may incorporate into their national law rules for prioritisation of complaints based on reviewable and publicly available criteria.</u>**

Presidency first compromise text	Drafting suggestions and Comments
	CZ (Comments): CZ: The aim of detailed rules for handling of complaints lies in the possibility of prioritising and planning regulatory action based on the actual impact of complaints and the resources available. Prioritisation shall be based on reviewable and publicly available criteria, without prejudice to the obligation to provide a reasoned effective response and subject to judicial review in every case. The powers of supervisory authorities to adopt planning instruments for the prioritisation and management of complaints should be expressly recognised. This would enable the DPAs more targeted supervisory activities based on evaluation of the level of risk, affects, type of processing, sector etc., while maintaining the capacity for individual assessment of each case. Priority should be given in particular to complaints that demonstrate a clear link to the core right to data protection or a high risk to rights and freedoms, affect many data subjects as well as other criteria FI (Drafting suggestions): **NEW 14a. In Article 83, paragraph 5, the following point is inserted:** **(f) any obligations pursuant to Articles 88a and 88b** FI (Comments): Finland considers it vital to ensure that the new provisions to the GDPR are subject to appropriate corrective measures, including administrative fines. Similar amendment should be proposed to Article 66(3) of the EUDPR. See **drafting suggestion bolded and underlined**. Taking account the nature of the proposed Articles 88a and 88b, Finland considers that the appropriate level of administrative fines would be up to 20

Presidency first compromise text	Drafting suggestions and Comments
	000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. Therefore, Finland proposes to add in Article 83(5) GDPR a new point concerning the infringements of obligations pursuant Articles 88a and 88b. See also EDPB-EDPS Joint Opinion, paras 107 and 117: *107. Proposed Article 88a GDPR and proposed Article 37 EUDPR cannot be implemented and enforced without the provision of supervisory powers. The EDPB and the EDPS therefore point out that it is necessary to provide for supervisory authorities' and the EDPS' fining powers for infringements of proposed Article 88a GDPR and Article 37 EUDPR as amended respectively, by including a reference to the provisions in Article 83(5) GDPR and Article 66(3) EUDPR.* *117. Lastly, similarly to the previous section, the EDPB and the EDPS point out that it is necessary to provide for supervisory authorities' and the EDPS' fining powers for infringements of proposed Article 88b GDPR and Article 37 EUDPR as amended respectively, by including a reference to the provisions in Article 83(5) GDPR and Article 66(3) EUDPR. Additionally, the EDPB and the EDPS also underline the need to ensure effective enforcement with regard to providers of web browsers and, if inclusion in scope were to be supported by the co-legislators based on the above recommendations, also to providers of operating systems.* NL (Drafting suggestions): **14a. Article 83 is amended as follows:** **(a) Paragraph 5, point d, is replaced with the following:**

Presidency first compromise text	Drafting suggestions and Comments
	‘(d) any obligations pursuant to Member State law adopted under Chapter IX **or to Articles 88a and 88b;** **(b) The following paragraph is added:** **10. This article applies accordingly to web browsers and other providers of software who infringe Article 88b(6), subject to the applicability of the maximum administrative fine referred to in paragraph 5.** NL (Comments): For reasons of legal certainty, NL proposes to add the threat of administrative fines for the new articles 88a and 88b GDPR, in accordance with §107 and 117 of the EDPB/EDPS Opinion. The Commission stated that elements of these articles rely on other GDPR provisions, that are subject to fines pursuant Article 83, e.g. lawfulness of processing, conditions of consent. However, these new articles provide for new elements as well. Therefore, proposes to indicate which level of GDPR administrative fines would apply to these articles. The amount of the fines connects with the existing obligations meant in Chapter IX GDPR. Furthermore, paragraph 117 of the EDPS/EDPB Opinion is incorporated in the new Article 83(10), by regulating effective enforcement with regard to providers of web browsers and other software providers, referred to in Article 88b(6).
15. After Article 88, the following articles are added:	CZ (Comments): CZ: Additionally, the scope of Art 83(5) should be extended and new point (f) should be added: “**specific processing situations pursuant to Articles 88a to 88c.** ”

Presidency first compromise text	Drafting suggestions and Comments
	These provisions are different from other articles on specific processing situations, because these provisions do not rely on Member State law. Therefore, the sanctions for breaches of Art. 88a-88c should be stipulated in the GDPR.
‘Article 88a	CZ (Comments): CZ: ***General comment: All obligations under Art. 88a-88c should be subject to sanctions.*** Simulatenously, we would like to better understand from the EC how it has considered **automotive** sector and impact of the proposed rules to the security, drivers assistance and development purposes of this sector. SI (Comments): In general cookies should be regulated by uniform standards and exceptions and should be subject to a uniform system of oversight. Furthermore, it remains unclear to what extent the provisions regarding the processing (storage) of personal data on the terminal equipment of natural persons will be relevant at all.
Processing of personal data in the terminal equipment of natural persons	CZ (Drafting suggestions): Processing of personal data in the terminal equipment of natural persons **in connection with the provision of publicly available electronic communications services in public communications networks** CZ (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	CZ: The proposed wording, considering the unclear scope of application (the meaning of "personal data already stored in the terminal equipment" in the context of GDPR as a general regulation of personal data proceesing as opposed to e-Privacy Directive, i.e. the processing of personal data in electronic communications), is too far-reaching. The scope and limits of the provision as formulated in this way are unclear. Such an approach could allow for blanket surveillance and interference with the privacy of end-users, contrary to Articles 7 and 8 of the Charter and the case-law of the Court of Justice. Following the clarification of the scope of the provision the wording shall be amended to include proper safeguards. DK (Comments): DK is concerned of the approach where provisions on accessing or storing personal data from terminal equipment are moved from the ePrivacy directive to GDPR, while provisions regarding accessing or storing of non-personal data from terminal equipment are maintained in the ePrivacy directive's Article 5(3). As a consequence, providers will have to adhere to two different sets of rules for accessing and storing data from terminal equipment, adding further complexity and legal uncertainty, undermining the purpose of an omnibus. Furthermore, as it may be difficult for providers to ascertain whether they are accessing personal or non-personal data, they may be obligated to follow the now stricter requirements for non-personal data (which does not have the same exemptions for consent as proposed for personal data), why the intentions with the new Article 88a of reducing cookie banners will not be realized. This problem should be addressed one way or another.
(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.	CZ (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
	(1) Storing of personal data, or gaining of access to personal data already stored, **in connection with the provision of publicly available electronic communications services in public communications networks ('personal communication data')** in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation. CZ (Comments): CZ: See above on more precise formulation. NL (Drafting suggestions): (1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation. **Subsequent processing of those personal data for the same purpose relies on the same consent.** NL (Comments): In accordance with §100 of the EDPS/EDPB Opinion, NL proposes to clarify this paragraph.
(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).	CZ (Drafting suggestions): (2) Paragraph 1 does not preclude storing of personal **communication** data, or gaining of access to personal **communication** data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard

Presidency first compromise text	Drafting suggestions and Comments
	the objectives referred to in Article 23(1)**, subject to conditions set in Article 23 that shall apply *mutatis mutandis*.** CZ (Comments): CZ: First, precise definition of relevant personal data is taken over from paragraph 1 by using short phrase. Second, reference to "objectives referred to in Article 23(1)" should be supplemented by reference to the safeguards provided for by Article 23. These safeguards include the legislative nature of a measure, the respect of the essence of the fundamental rights and freedoms and the necessity and proportionality requirements in paragraph 1, and concrete elements of the legislative measure required by paragraph 2 where relevant. Third, because the Article 23(1) refers to limitation of particular rights provided in specific provisions of GDPR, the reference should be to conditions that apply "mutatis mutandis". Legislative technique of Regulation 2019/1381 is used. NL (Drafting suggestions): ~~(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).~~ **In article 23, paragraph 1, "Articles 12 to 22 and Article 34" is replaced by "Articles 12 to 22, 34 and 88a".** NL

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): Article 88a(2) concerns restrictions that can be made by Member State law. Since Article 23 GDPR is the general article concerning restrictions by Union or Member State law, NL considers it more logical and consistent to include a reference to Article 88a in Article 23 GDPR instead.
(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:	CZ (Drafting suggestions): (3) Storing of personal **communication** data, or gaining of access to personal **communication** data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following **purposes**: CZ (Comments): CZ: CZ is supportive of the text but can accept more precise reference to "purposes" as suggested by Joint Opinion of EPDB and EDPS. FI (Comments): Finland has previously commented on the "*the subsequent processing*" and welcomes the Presidency to consider the EDPB-EDPS Joint Opinion (paras 99-100). *100. The EDPB and the EDPS note that proposed Article 88a(1) and (2) GDPR and proposed Article 37(2) and (3) EUDPR take a different approach than Article 88a(3) GDPR and Article 37(4) EUDPR, as the former do not regulate the lawfulness of subsequent processing. To ensure legal certainty and to simplify compliance, the EDPB and the EDPS recommend to regulate the subsequent processing of personal data accessed or stored in terminal equipment based on consent or Union or Member State law in a similar*

Presidency first compromise text	Drafting suggestions and Comments
	manner as under proposed Articles 88a(3) GDPR and 37(4) EUDPR. This would entail that subsequent processing of personal data stored or accessed in terminal equipment, for the same purpose, would rely on the same consent or provision of Union or Member State law allowing the personal data to be initially stored or accessed. Proposed Recital 44 should also be amended accordingly, also clarifying that where processing relies on consent under Article 88a(1) GDPR and Article 37(2) EUDPR, the consent should clearly encompass both the access to the terminal equipment and the subsequent processing carried out for the same purpose. Subsequent processing of personal data for a purpose other than that for which the personal data has been stored or accessed will be considered as further processing, as referred to under Article 6(4) GDPR. NL (Drafting suggestions): (3) **Notwithstanding paragraph 1, the** storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, and subsequent processing, shall be ~~lawful~~ **permissible where it is based upon a legal basis in accordance with Article 6(1) other than consent, and** to the extent it is **strictly** necessary for any of the following **purposes**: NL (Comments): NL proposes to link the exceptions, meant in Article 88a(3), to the legal bases in Article 6(1) GDPR. These exceptions, especially the new ones (Art. 88a(3) point c and d), are formulated in broad terms and could otherwise imply blanket lawfulness for storage of or access to information on terminal equipment for these purposes. Linking these exceptions to Article 6(1) instead, preserves the required balancing test for legitimate interests and, importantly, ensures that controllers must properly consider data subjects' rights and interests prior to their processing. In addition, a substantial body of

Presidency first compromise text	Drafting suggestions and Comments
	case law has already been developed around the concept of legitimate interest. Therefore, linking these exceptions contributes to legal certainty for controllers, as they are able to rely on existing case law for these purposes. The words "purposes" and "strictly" are added in accordance with paragraphs 99 and 101 of the EDPB/EDPS Opinion.
(a) carrying out the transmission of an electronic communication over an electronic communications network;	
(b) providing a service explicitly requested by the data subject;	FI (Comments): See EDPB-EDPS Joint Opinion, para 101: *101. The EDPB and the EDPS note that compared to current Article 5(3) ePrivacy Directive, proposed Article 88a(3)(b) GDPR and proposed Article 37(4)(b) EUDPR contain a broadened exception to consent for access to storage of personal data in terminal equipment. Namely, pursuant to the Proposal, no consent is required for 'providing a service explicitly requested by the data subject', while under Article 5(3) ePrivacy Directive, this exception is limited to the provision of an information society service. In addition, proposed Article 88a(3)(c)–(d) GDPR and proposed Article 37(4)(c)–(d) EUDPR contain new exceptions for audience measurement and security purposes accordingly103 . In this regard, the EDPB and the EDPS recommend to clearly delimit the processing in scope of such exceptions to what is strictly necessary*
(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;	CZ (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	CZ: CZ believes that this exemption in point c) should be primarily limited to the controller (and processor) of a service requested by data subject (however CZ is open to further expert discussions). DK (Comments): Can the Commission clarify whether media services providers can utilise this exemption for gathering data from terminal equipment to measure the audience of their services while adhering to the standards set out in the European Media Freedom Act on independent audience measurement? Can the Commission clarify whether it is possible for a third party to conduct independent audience measurements when the third party has legal status of a "processor" as foreseen in preamble 44? FI (Drafting suggestions): c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service **or mandated joint controller** solely for **their** own use; FI (Comments): Finland welcomes the Commission's proposal to exclude media service providers from the centralized consent regime. The proposal recognizes the importance of digital advertisement revenues for independent journalism as an indispensable pillar of a democratic society. In order to fully realize the benefits of the media exemption, it should be clarified that the exemption also covers third-party cookies when used in connection with media services.

Presidency first compromise text	Drafting suggestions and Comments
	Information obtained through audience measurement serves as the currency for advertising sales, and the measurement data is also important for media policy preparation and decision-making. Traditional media audience measurement is based on measurement systems developed within self-regulatory organisations, such as industry-wide committees, in accordance with standards approved by the sector. Online platforms, in turn, carry out their audience measurement themselves or offer their own audience measurement systems on the market, which do not follow commonly accepted industry standards or best practices. For media companies' advertising sales, it is essential that third-party research organisations conducting audience measurement independently and in line with industry standards can continue to carry out such measurement in the future. Efforts have been made to improve the transparency and comparability of audience measurement between traditional media audience measurement and the proprietary audience measurement systems of online platforms through the European Media Freedom Act. Therefore, with regard to the legal basis for processing audience measurement data, it would be appropriate to take into account the consistency of the Union's legislative framework, and to ensure that cookie regulation also enables the continuation of standardised audience measurement within the media sector. The recital 44 paragraph 3 notes that "the controller, such as a media service provider, may mandate a processor, such as a market research company, to carry out the processing on its behalf". However, the independent audience measurement provider typically operates as a joint controller under the GDPR. For the sake of clarity, the article text should be amended to specifically allow for the use of joint controller. IT (Comments): The actual text appears to conflict with Article 24 (1) of the EMFA Regulation, which provides a series of provisions regarding audience

Presidency first compromise text	Drafting suggestions and Comments
	measurement for all (proprietary audience measurement and non-proprietary audience measurement) providers of audience measurement systems. In particular, the exemption rule under Article 88a of the Digital Omnibus appears to conflict with the principles of comparability and verifiability of audience data under Article 24 of the EMFA between different audience measurement systems, since data from measurement systems developed in compliance with industry standards within self-regulatory bodies, such as JICs or research companies, would be less significant and reliable than data from proprietary audience measurement system providers. Hence, some sort of exemption should be foreseen in the text also for self-regulatory bodies, such as JICs or research companies. NL (Drafting suggestions): (c) creating aggregated information about the usage of an online service **during the use of that service by the data subject.** to measure the audience of such a service, where it is carried out by the controller **providing** ~~of~~ that online service **or by a processor on behalf of this provider** solely for its own use **to obtain insight into the performance and use of the online service in an aggregated and general manner**; NL (Comments): NL proposes to make this exemption more precise and limited, by the addition that it only applies during the use of the service by the data subject. Furthermore, this paragraph is clarified in accordance with the EDPB/EDPS Opinion (§102).. SI (Drafting suggestions): **Amend**

Presidency first compromise text	Drafting suggestions and Comments
	SI (Comments): This exemption should be limited only to a specific service and the individual using this service, and only in cases where the individual can reasonably expect such processing. "Aggregated information" should be further clarified in a recital.
(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.	CZ (Comments): CZ believes that this exemption in point d) definitely ought to be further specified. We are flexible as to the method – we could include specific examples or refer to information technology security or to elaborate this issue in a recital. Specifically, we present to the Presidency following examples that could be considered legitimate uses of security exemption: Security of the service provided by the controller: • Anti-fraud and anomaly detection: Storing identifiers to detect suspicious behavior (e.g., unusual login from another country, changes in behavior patterns indicating account compromise) • Rate limiting: Cookies/fingerprinting to protect against DDoS attacks and brute-force login attempts • CSRF tokens: Protection of forms against cross-site request forgery and similar attacks • Session integrity: Control mechanisms to detect "session hijacking" or "session fixation"

Presidency first compromise text	Drafting suggestions and Comments
	• Bot detection: Identification of automated access threatening service availability Security of the end user's device: • Phishing warning: Systems warning users about compromise of their devices • TLS/certificate verification: Data necessary to verify secure connection Important note: The "necessity" test must be met - an alternative solution without access to personal data would not be sufficiently effective. And the service must be "requested" by the data subject. FI (Drafting suggestions): (d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service. FI (Comments): See EDPB-EDPS Joint Opinion, para 103. *103. In addition, proposed Article 88a(3)(d) GDPR regarding lawfulness of processing for maintaining or restoring the security of a service* ***should be further specified to mean IT security and data protection security****. - - A provider of security patches should in general therefore be able to install the strictly necessary security updates without consent from the user. However,*

Presidency first compromise text	Drafting suggestions and Comments
	this should only be allowed to the extent that (i) the security updates are discretely packaged and do not in any way change the functionality of the software on the terminal equipment (including the interaction with other software or settings chosen by the user), (ii) the end-user is informed in advance each time an update is being installed, and (iii) the user has the possibility to turn off the automatic installation of these updates. IT (Drafting suggestions): **Litt.(e) should be added as follows:** **e) less intrusive forms of advertising online, namely contextual advertising based on individual current visit to single web page with no retention of data related to the individual online activity** IT (Comments): It would be appropriate to specify, either on the provision or on a recital, that the security to be maintained or restored refers to IT and data protection. Moreover, it could be considered to add, as suggested by the EDPB/EDPS Opinion, an additional exception for contextual advertising, provided that the exception is strictly limited and includes appropriate safeguards to mitigate the risks for the rights and freedom of the individual SI (Drafting suggestions): **Amend** SI (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	This exemption should be limited to data protection and IT security and should only reflect a specific service provided and used by an individual. "IT security" should be further clarified in a recital.
	CZ (Drafting suggestions): After (d), the following points are added: **'(e) contextual advertising and related limitation of advertisement display, audience measurement and preventing fraudulent misrepresentation of audience, unless at least one of the following applies:** **(i) the processing is likely to result in a risk to the rights and freedoms of natural persons;** **(ii) the processing involves profiling;** **(iii) personal data are stored at the time when the electronic communication service is not actively used;** **(iv) personal data are connected with past or future activity of the data subject.** CZ (Comments): CZ suggests adding new exemptions concerning activities that are not based on profiling, i.e. covering low- risk to the rights and freedoms, non- profiling activities that do not involve any retention of personal data beyond the user's active session nor any link to past or future behaviour. This suggestion is inspired by the EDPB/EDPS joint opinion (point 104) which emphasises the need to create incentives to use less- intrusive forms of online advertising and aimed to make the rules more proportionate, i.e. allowing some forms of targeted advertising, which is crucial for European publishers and service providers.

Presidency first compromise text	Drafting suggestions and Comments
	CZ remains open to work around our suggestion esp. concerning necessary safeguards. IE (Drafting suggestions): (e) providing contextual advertising based on an individual current visit to a single web page or based on a single search query and that involves no retention or link with the individuals past or future activity. IE (Comments): Ireland agrees with the recommendation of the EDPB and EDPS and supports inclusion of an additional exception for contextual advertising provided that the exception is clearly limited and included necessary safeguards.
(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:	CZ (Drafting suggestions): Where storing of personal **communication** data, or gaining of access to personal **communication** data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply: CZ (Comments): CZ: See above on terminology. NL (Drafting suggestions): (4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply **in addition to Article 7**: NL

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): NL proposes to include a reference to Article 7 GDPR to clarify these conditions still apply.
(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;	NL (Drafting suggestions): (a) the data subject shall be able to **reject** ~~refuse~~ requests for consent **and withdraw consent** in an easy and intelligible manner with a single-click button or equivalent means; NL (Comments): In this paragraph should be included that the data subject shall also be able to withdraw consent in accordance with Article 7 GDPR.
(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;	
(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.	CZ (Comments): CZ: Could the EC explain based on which criteria/assessment it has suggested period of 6 months, and for example not a period shorter? We note that in some MS the current practice is to work with the "strictly necessary period", with case-by-case decision making by the responsible DPA. Has this approach been considered by the EC as well? NL (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
	c) if the data subject **rejects** ~~declines~~ a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.
This paragraph also applies to the subsequent processing of personal data based on consent.	CZ (Drafting suggestions): This paragraph also applies to the subsequent processing of personal **communication** data based on consent. CZ (Comments): CZ: See above on terminology. FI (Comments): Finland has previously commented on the "*the subsequent processing*" and welcomes the Presidency to take into account the EDPB-EDPS Joint Opinion (paras 99-100).
(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]	
Article 88b	
Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons	CZ (Drafting suggestions): Automated and machine-readable indications of data subject's choices with respect to processing of personal **communication** data in the terminal equipment of natural persons CZ

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): CZ: See CZ comments to Art. 88a on the scope of this notion, which has to be uniform for both provisions. DK (Comments): We take note of concerns expressed by other Member States and many stakeholders regarding this article. We would ask the Commission to kindly help clarify: - Many stakeholders caution of the consequences to the ad-supported web and -economy. What consequences for the ad-supported web and -economy do the Commission foresee as an effect of the obligatory central consent mechanisms as envisioned in Article 88b? - The Commission's aim with the Digital omnibus is to simplify and reduce burdens for companies, however, this article is introducing new obligations on providers of web browsers that are not SMEs, as they are obligated to provide the technical means to ensure that all online interfaces allow data subjects to give consent or decline requests for consents through automated and machine-readable means. How is this better suited for an omnibus proposal than a revision which would be accompanied by an impact assessment? - Can the Commission clarify how this article corresponds with the requirement that consent must be "specific", "informed" and "unambiguous" according to Article 4(11) in the GDPR? IE (Comments): Ireland has concerns that Article 88b may not in practice achieve its objective of reducing 'banner fatigue', and that its addition could introduce legal uncertainty and add a significant cost burden on businesses, with SMEs

Presidency first compromise text	Drafting suggestions and Comments
	disproportionately affected, all of which is contrary to the broader objectives of the simplification agenda. IE also notes that other policy options may exist to better achieve the desired objective. In light of these concerns, IE preference at this stage is for further analysis, from a legal and technical perspective, as to how best to achieve the objective of reducing 'banner fatigue'. This may, for example, be possible through further clarification of exemptions in Article 88a.
(1) Controllers shall ensure that their online interfaces allow data subjects to:	SI (Comments): It should be clarified which controllers are subject to this provision, e.g., website providers, app providers, and web browser providers.
(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;	NL (Drafting suggestions): (a) Give consent **for specific categories of data processing** through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled; NL (Comments): NL questions how and if giving (general) consent under the proposed Article 88b(1)(a) GDPR can be considered "specific" and lawful according to Recital 32 GDPR and Articles 7 and 4(11) GDPR. Therefore, the NL proposes to further specify how this consent has to be given, for example for each purpose and for each controller or for specific categories of data processing.
(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.	NL

Presidency first compromise text	Drafting suggestions and Comments
	(Drafting suggestions): (b) decline a request for consent **or** ~~and~~ exercise the right to object pursuant to Article 21(2) through automated and machine-readable means. NL (Comments): This clarifies that the declination of a request does not necessarily have to be combined with an objection.
	NL (Drafting suggestions): **(c) withdraw consent through automated and machine-readable means.** NL (Comments): With this paragraph, NL proposes to include that the data subject shall also be able to withdraw consent in accordance with Article 7 GDPR.
(2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1.	NL (Drafting suggestions): (2) Controllers **who access or store data in the terminal equipment of data subjects** shall respect the choices made by data subjects in accordance with paragraph 1. NL (Comments): In accordance with §111 of the EDPB/EDPS Opinion, NL proposes to clarify this paragraph and the corresponding recital 45.
(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.	DK

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): Many stakeholders, including the media industry, have expressed concerns regarding this exemption, stating that it will have the reverse effect than the stated objective. Stakeholders point to how - The article does not take account for the fact that most media service providers are reliant on a network of technology partners acting as data controllers, and the media service providers cannot monetize their content or data without these third parties. - There is a risk of negative reactions from the users, as users as a consequence will primarily be faced with cookie banners on websites belonging to media service providers. Users could be more likely to seek news on other services, e.g. online platforms. It would be helpful if the Commission could help clarify whether these concerns are well funded? IT (Drafting suggestions): ~~Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.~~ IT (Comments): The need to alleviate consent fatigue is applicable to media as well. Moreover, the need to treat media as other service providers is also due to the fact that the processing of data for advertising purposes when accessing media is very often carried out by third parties which provide services embedded in media websites NL (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
	(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service. **Article 88a remains fully applicable to these providers.** NL (Comments): With this addition, NL proposes to clarify that an exemption from the obligation to respect a signal transmitted through automated means indicating consent preferences of a user does not mean an exemption from asking consent, as the Commission has stated. However, NL makes a study reservation about the exemption for media service providers regarding the impact on solving the cookie-fatigue. SI (Drafting suggestions): ~~(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.~~ SI (Comments): **Delete** Controllers that are media service providers should not be exempted from obligations set in this Article. Furthermore, safeguards should be added to the article to address the aggressive use of cookies by media service providers, as observed in practice, including in the provision of media services.
(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices.	SI (Comments): We propose to set the deadline for the adoption of such standards.

Presidency first compromise text	Drafting suggestions and Comments
Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.	
(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].	
(6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.	CZ (Comments): CZ: We support question raised during the last examination of the text during the AGS meeting on 27 February by the NL concerning the communication between the web browser and the website and technical explanation on how the EC expects that the interaction will work, incl. the enforcement, which we do not think has been replied by the EC. In this regard, we would like to invite the EC to elaborate on the technical process more in details. We would also like to support suggestion by some other MS to organize a technical workshop on the articles 88a and 88b of the digital omnibus, to better understand the EC's intention of this part of the proposal. NL (Drafting suggestions): (6) Providers of web browsers~~, which are not SMEs,~~ **and other providers of software used in the terminal equipment used by natural persons** shall provide the technical means to allow data subjects to give their consent~~, and~~ to refuse a request for consent**, to withdraw consent,** and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article. NL

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): NL proposes to include that the withdrawal of consent in accordance with Article 7 GDPR is facilitated. The exemption for SMEs is deleted in accordance with paragraph 114 of the EDPB/EDPS Opinion. The paragraph is extended to other software providers in accordance with paragraph 115 of the EDPB/EDPS Opinion, which would include consumer mobile and desktop operating systems.
(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].	
Article 88c	CZ (Drafting suggestions): ~~**Article 88c**~~ **Article 6a** CZ (Comments): CZ: If adopted, Article 88c GDPR should be moved to Article 6a GDPR, where it fits more systematically. It regulates the legal basis for processing personal data for AI purposes. NL (Drafting suggestions): ~~Article 88c~~ SI (Comments): **Delete**

Presidency first compromise text	Drafting suggestions and Comments
	We are in favour of deleting Article 88c, because it is inconsistent with the logic and the protection system established by the GDPR, has no added value in terms of providing an additional ground for processing. Such processing may already be pursued for legitimate interest in accordance with Article 6(1)(f) of GDPR, which is also in line with the general principle of technologic neutrality.
Processing in the context of the development and operation of AI	NL (Drafting suggestions): ~~*Processing in the context of the development and operation of AI*~~
Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	CZ (Drafting suggestions): Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning **and subject to the conditions** of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, ~~**and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.**~~ CZ (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	  CZ prefers clear and simple reference to all conditions of Art. 6(1)(f) where this legal basis is relied upon. Simplification is not achieved by confusion. These particular phrases are not necessary if the whole Art. 6(1)(f) is clearly referred to (see above). FI (Drafting suggestions): Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) **[in this Regulation]** ~~**of Regulation (EU) 2016/679, where appropriate,**~~ except ~~**where other Union or national laws explicitly require consent, and**~~ where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child **and except where other Union or national laws explicitly require consent. The processing of personal data in the context of the development and operation of an AI system may also be based for the performance of a**

Presidency first compromise text	Drafting suggestions and Comments
	task carried out by public authorities in the public interest pursuant to Article 6, paragraph 1, point (e) and paragraph 2. FI (Comments): Finland proposes to clarify the proposed Article 88c. See **drafting suggestions striken, underlined and bolded (optional in brackets)**. **First**, it is necessary to ensure that the controllers always do the three-step test and therefore "where appropriate", should be deleted. See EDPB-EDPS Joint Opinion, para 41. **Second**, as a technical remark, it is not necessary to refer to the GDPR ("Regulation (EU) 2016/679") as this provision is going to be added in the GDPR. If a reference to the GDPR is needed (as there is a reference to another Regulation), alternatively the wording could be "in this Regulation". See optional drafting suggestion in brackets. **Third**, the except for consent should be, for legal clarity, transferred to the end of the sentence. **Last**, it should be clarified and added, that public authorities may rely on public interest for the processing of personal data in the context of the development and operation of an AI system. Finland clarifies that this clarification is needed, as the GDPR states that 6(1)(f) of the GDPR shall not apply to processing carried out by public authorities in the performance of their tasks. Such processing shall comply with the provisions of Articles 6(1)(e) and 6(2) of the GDPR. Finland considers that this clarification should be made at least in the recitals. IT (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
	Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning **and conditions** of Article 6(1)(f) of Regulation (EU) 2016/679, **and in compliance with the requirements set forth by the same Article 6,** where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. IT (Comments): It would be important to refer to the requirements set forth by Article 6(1)(f) to provide that controllers still have to carry out the necessary three-step case-by-case assessment to verify that they can lawfully rely on Article 6(1)(f) (as recommended by the EDPB/EDPS in their joint Opinion). NL (Drafting suggestions): ~~Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.~~ NL

Presidency first compromise text	Drafting suggestions and Comments
	(Comments): - The NL agrees with the EDPB/EDPS Opinion (§39) that Article 88c is not necessary and that it does not bring any legal clarification. - Furthermore, NL notes that it risks a deterioration of the legal position of data subjects by giving a heavy weight to legitimate interest as a legal basis for development and operation of AI. The current GDPR contains no article at all stating that a specific data processing or application can lead to a legitimate interest. As a result, Article 88c could give the impression that this legal basis is given by default, without a necessity test and the associated balancing test of interests. There are concerns about this article among a majority of the Dutch House of Representatives, which adopted a motion related to this article. Article 88c would pre-determine the outcome of this tests by apparently declaring AI development and operation a legitimate interest by default. It would become easier for AI companies to justify their activities under a legitimate interest. - The easier it is for AI companies to rely on a legitimate interest as a basis for personal data processing, the less often they would need consent from data subjects as a basis. - If consent from data subjects is not required, it is more difficult for them to exercise their rights, because they have less insight into the data processing, and it is more difficult to have personal data erased afterwards. Once data have been processed in major language models, it can be difficult to honor requests for access, rectification, deletion, and objection. - Especially when data are not collected directly from data subjects, there is a risk that data subjects often do not know when or by whom their data is being used for AI training purposes, or that they would have to object to an unknown number of companies to prevent the processing of their personal data.

Presidency first compromise text	Drafting suggestions and Comments
	- By apparently declaring AI development and operation a legitimate interest by default, the burden could shift to data subjects if they would object to the data processing. - Article 88c risks benefiting existing AI companies who (already) possess data sets *with personal data* more than (new) AI companies who do not have data sets with personal data and who do not intend to use personal data (without consent of data subjects). - Article 88c deviates from EDPB opinion 28/2024, for example because it fails to provide that the reasonable expectations of data subjects must be taken into account, such as whether the personal data were already public and whether there is a relationship between the data subject and the controller. In addition, while the aim of this article is to clarify the current GDPR rules, it raises new questions, among others, regarding the "unconditional right to object" and the relation to EDPB Opinion 28/2024. SI (Drafting suggestions): ~~Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.~~ SI (Comments): **Delete**

Presidency first compromise text	Drafting suggestions and Comments
Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'	FI (Drafting suggestions): Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects ~~**and providing data subjects with an unconditional right to object to the processing of their personal data**~~. **The data subject shall also have an unconditional right to object to processing of personal data concerning him or her, which is based on point (f) of Article 6(1) [of this Regulation].** FI (Comments): Finland proposes to clarify the unconditional right to object, based on the EDPB-EDPS Joint Opinion (para 42). See **drafting suggestions striken, underlined and bolded**. See also comments and drafting suggestions from the recitals. **Finland also welcomes the Presidency to further clarify what "enhanced transparency" means**. In this regard Finland point out the EDPB-EDPS Joint opinion (para 43). *43. Thirdly, 'enhanced transparency' is also mentioned as a mitigating measure 51 without providing clarification on the extent of this transparency obligation. The EDPB and the EDPS recommend clarifying this aspect by specifying that it means providing additional information compared to the information that has to be provided according to Articles 13 and 14 GDPR.* IT

Presidency first compromise text	Drafting suggestions and Comments
	(Drafting suggestions): **Without prejudice of the obligations provided for by Regulation (EU) 2016/679,** any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects**, by means of additional information compared to the information that has to be provided pursuant to Articles 13 and 14**, and providing data subjects with an unconditional right to object to the processing of their personal data. **Such right should be brought to the attention of data subjects, whenever possible and sufficiently in advance in respect of the processing of their personal data, in the context of the development and operation of AI, to enable them to exercise it from the outset.** IT (Comments): The additional suggestions aim at: - Avoiding possible confusion between the mitigating measures introduced by the proposal and the measures that controllers are obliged to adopt in compliance with the GDPR - clarifying the scope of the enhanced transparency obligations and highlighting that the enhanced transparency refers to additional information compared to what is already provided by Article 13 and 14 - raising the awareness of the data subject on the existence of the unconditional right to object. Finally, one may consider to bring up to Article 21 the reference to the unconditional right to object.

Presidency first compromise text	Drafting suggestions and Comments
	NL (Drafting suggestions): ~~Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'~~ SI (Drafting suggestions): ~~Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'~~ SI (Comments): **Delete**
	IT (Drafting suggestions):

Presidency first compromise text	Drafting suggestions and Comments
	Amendment to Article 89(2) "Member States and Union law may provide that the rights referred to in Articles 15 to 22 shall not apply, in whole or in part, where their exercise is likely to render impossible or seriously impair the achievement of scientific or technological research purposes."
Article 4	
Amendments to Regulation (EU) 2018/1725 (EUDPR)	FI (Comments): Finland expresses that the above considerations on GDPR apply with respect to the EUDPR. NL (Comments): **The NL textual proposals regarding the GDPR apply mutatis mutandis to the EUDPR.**
Regulation (EU) 2018/1725 is amended as follows:	
1. Article 3 is amended as follows:	
(a) in point 1, the following sentences are added:	
'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a	

Presidency first compromise text	Drafting suggestions and Comments
potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'	
(b) point 25 is replaced by the following:	
'(25) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;'	
(c) the following points are added:	
'(27) 'mobile application' means a mobile application as defined in Article 3(2) of Directive (EU) 2016/2102;	
(28) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065;	
(29) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'	
2.Article 4 (1)(b) is replaced by the following:	
'(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 13, be considered to be compatible with the initial purposes,	

Presidency first compromise text	Drafting suggestions and Comments
independent of the conditions of Article 6 of this Regulation, ('purpose limitation');'	
3.Article 10 is amended as follows:	
(a) in paragraph 2, the following points are added:	
'(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 4. .	
(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.'	
(b) the following paragraph 4 is added:	
'4. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.'	
4. in Article 14, paragraph 5 is replaced by the following:	

Presidency first compromise text	Drafting suggestions and Comments
'5. Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 35 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 17 because the data subject abuses the rights conferred by this Regulation for purposes other than the protection of their data, the controller may refuse to act on the request. The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.'	
5. in Article 15 the new paragraph 5 is added:	
'5. When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 13 or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.'	
6. in Article 24 paragraphs 1 and 2 are replaced by the following:	
'1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision:	
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means;	

Presidency first compromise text	Drafting suggestions and Comments
(b) is authorised by Union law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or	
(c) is based on the data subject's explicit consent.'	
7. in Article 34, paragraph 1 is replaced by the following	
'1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor. Where the notification to the European Data Protection Supervisor is not made within 96 hours, it shall be accompanied by reasons for the delay.'	
8. In Article 37 the following paragraphs are added:	
'(2) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.	
(3) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union law within the meaning of, and subject to the conditions of Article 5, to safeguard the objectives referred to in Article 25(1).	
(4) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and	

Presidency first compromise text	Drafting suggestions and Comments
subsequent processing, shall be lawful to the extent it is necessary for any of the following:	
(a) carrying out the transmission of an electronic communication over an electronic communications network;	
(b) providing a service explicitly requested by the data subject;	
(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;	
(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.	
(5) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:	
(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;	
(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;	
(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.	

Presidency first compromise text	Drafting suggestions and Comments
This paragraph also applies to the subsequent processing of personal data based on consent.	
(6) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]]	
(7) Controllers shall ensure that their online interfaces allow data subjects to:	
(a) give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;	
(b) decline a request for consent through automated and machine-readable means.	
(8) Controllers shall respect the choices made by data subjects in accordance with paragraph 7.	
(9) Online interfaces of controllers which are in conformity with harmonised standards or parts thereof referred to in paragraph 4 of Article 88b of Regulation (EC) 2016/679 shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 7.	
(10) Paragraphs 7 to 9 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].	
(8) Article 39 is amended as follows:	
(a) Paragraph 4 is replaced by the following:	

Presidency first compromise text	Drafting suggestions and Comments
'4. The lists, the template and methodology adopted by the Commission and referred to in paragraph 6a of Article 35 of Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation.'	
(b) Paragraphs 5 and 6 are deleted.	
(9) the following article is added:	
'Article 45a	
The common criteria adopted by the Commission and referred to in article 41a of the Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation.'	
Article 5	
Amendments to and Directive 2002/58/EC (ePrivacy Directive)	CZ (Comments): CZ: It remains unclear why the regimes for personal and non personal data should be differentiated, i.e. keeping part of the rules in the GDPR and the other in ePrivacy Directive. **In this regard, we would like to suggest that the simplification would be rather fulfilled if the whole framework is placed in one set of rules.** This would also improve legal clarity and certainty **and might react to some concerns among other MS possibly in a clearer way than clarifying what is meant by non-personal data.** In case that, for any reason, the rules under the GDPR and ePD would be kept for personal/non-personal data, ePD framework should be accompanied by examples of what might constitute non-personal data. CZ is of the opinion that clarifying the co-legislators will in the ePrivacy Directive and art. 5(3), **which has been understood extensively by the**

Presidency first compromise text	Drafting suggestions and Comments
	stakeholders and in fact has been the main reason behind introducing the omnipresent cookie banners, would be an important contribution of the whole omnibus and solution of a current situation given the media exemption, i.e. the fact that cookies banners might remain present.
Directive 2002/58/EC is amended as follows:	
1. Article 4 is deleted;	SI (Comments): The Republic of Slovenia opposes the repeal of Article 4 of Directive 2002/58/EC, as this would result in reduced regulation in the field of security of electronic communications services. The security of processing should remain regulated within the framework of the protection of privacy in electronic communications.
2. After Article 5(3), the following subparagraph is added:	NL (Drafting suggestions): **2. Article 5(3) is replaced with the following:** ~~After Article 5(3), the following subparagraph is added:~~
'This paragraph shall not apply if the subscriber or user is a natural person, and the information stored or accessed constitutes or leads to the processing of personal data.'	NL (Drafting suggestions): 3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with **Regulation (EU) 2016/679** ~~Directive 95/46/EC~~, inter alia, about the purposes of the processing. ~~This shall not prevent any technical storage or access for the sole purpose of~~

Presidency first compromise text	Drafting suggestions and Comments
	~~carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.~~ **Member States shall provide by law that:** **a. This paragraph shall not apply if the storing or accessing of the information constitutes the processing of personal data;** **b. The exemptions to consent referred to in Article 88a(3) of Regulation (EU) 2016/679 apply accordingly to this paragraph;** **c. The designation of the competent data protection supervisory authority for Article 88a applies accordingly to this paragraph.** NL (Comments): NL proposes to simplify the relationship between Article 5(3) ePD and Article 88a GDPR, by harmonising the exceptions to the consent requirement and by assigning one supervisory authority. The aim of this is to avoid differences between the cookie rules in the ePD and GDPR. A further harmonisation could be considered by inserting into Article 5(3) ePD that Article 88b GDPR (Automated and machine-readable indications of data subject's choices) applies accordingly to cookies without personal data. SI (Comments): The Republic of Slovenia partially welcomes the amendment to Article 5(3) of Directive 2002/58/EC, which consolidates the provisions on the processing of personal data in terminal equipment with the proposed amendments to the GDPR, as this ensures a uniform legal framework for natural persons. Nevertheless, we call for caution when it comes to extending the scope of Directive 2002/58/EC. The exception in Article 5(3) of Directive 2002/58/EC, which refers to the provision of information society services

Presidency first compromise text	Drafting suggestions and Comments
	requested by an individual, is extended in accordance with proposal 88a (3) of GDPR to the provision of any service requested by an individual. Consequently, the Republic of Slovenia draws attention to the need for greater clarity in the wording of the exceptions in 88a(3) of the GDPR. Proposed amendment to Article 5(3) of the Directive 2002/58/EC may create inappropriate asymmetry: while personal data from terminal equipment will, in accordance with the proposal, be newly regulated in the GDPR (with prescribed exceptions where the consent of natural persons is not required), non-personal (anonymous) data from terminal equipment will still be subject to stricter regulation under Directive 2002/58/EC.
Article 10 **Repeals and transitory clauses**	FI (Comments): Finland is open to discuss Article 10 on the basis of comments made by other Member States.

1. Regulation 2019/1150/EU is repealed with effect from [date = entry into application of this Regulation].	BE (Drafting suggestions): 1. Regulation 2019/1150/EU is **partially** repealed with effect from [date = entry into application of this Regulation]. BE (Comments): Belgium believes certain P2B provisions to be essential safeguards for SMEs, we therefore propose to maintain them on a permanent basis, and not only until 31 December 2032. IE (Drafting suggestions): 1. Regulation 2019/1150/EU is **partially** repealed with effect from [date = entry into application of this Regulation]. IT (Drafting suggestions): 1. Regulation 2019/1150/EU is **partially** repealed with effect from [date = entry into application of this Regulation]. IT (Comments): ITALY believes certain P2B provisions to be essential safeguards for SMEs, we therefore propose to maintain them on a permanent basis, and not only until 31 December 2032. NL (Drafting suggestions): Regulation 2019/1150/EU is **partially** repealed with effect from [date = entry into application of this Regulation]. NL (Comments):

Presidency first compromise text	Drafting suggestions and Comments
	The Netherlands insists that a more targeted and proportionate approach is necessary to ensure continued protection of SMEs in their commercial relation with online platforms. We believe certain P2B provisions to be essential safeguards for SMEs, we therefore propose to maintain them on a permanent basis, and not only until 31 December 2032. The unique protective function of the P2B for those entrepreneurs in the Netherlands is reflected in the number of complaints and tip-offs received on non-compliant platforms by the Dutch competent authority for the P2B. The Netherlands Authority for Consumers and Markets (ACM) has been authorized to monitor and enforce compliance with the P2B since November 8, 2024. The ACM received a total of approximately 190 P2B-labelled complaints between 2024 and 2025. At least 65 of those complaints specifically concern issues relating to the suspension, restriction or termination of an account (Article 4) and the handling of complaints (Article 11). In addition, the ACM has also received more than 40 complaints concerning differential treatment (Article 7) and ranking (Article 5). Other complaints relate to the transparency of terms and conditions (Article 3) and other provisions.
2. By way of derogation from paragraph 1, the following provisions shall continue to apply until 31 December 2032:	BE (Drafting suggestions): – 2. **In accordance with** ~~By way of derogation from~~ paragraph 1, the following provisions shall continue to apply ~~until 31 December 2032~~: IE (Drafting suggestions): 2. **In accordance with** ~~By way of derogation from~~ paragraph 1, the following provisions shall continue to apply ~~until 31 December 2032~~:

Presidency first compromise text	Drafting suggestions and Comments
	IT (Drafting suggestions): 2. **In accordance with** ~~By way of derogation from~~ paragraph 1, the following provisions shall continue to apply ~~until 31 December 2032:~~ NL (Drafting suggestions): **In accordance with** paragraph 1, the following provisions shall continue to apply
	BE (Drafting suggestions): **(-a) Article 1;** BE (Comments): Article 1 must be maintained because it sets out the scope and subject matter of the P2B Regulation, which are necessary elements for the proper application of the other provisions that remain in force. CZ (Drafting suggestions): **Article 1** CZ (Comments): CZ: Article 1 of the P2B Regulation establishes the personal and territorial scope of the P2B Regulation, together with the relationship to other Union law and national rules. The determination of the scope of a legal norm is a fundamental prerequisite for its validity, and it is therefore crucial that Article 1 of the P2B Regulation shall be retained, as otherwise it would not be possible to enforce the obligations under the P2B Regulation at all.

Presidency first compromise text	Drafting suggestions and Comments
	IT (Drafting suggestions): **(-a) Article 1;** IT (Comments): Article 1 must be maintained because it sets out the scope and subject matter of the P2B Regulation, which are necessary elements for the proper application of the other provisions that remain in force. NL (Drafting suggestions): **(-a) Article 1;** NL (Comments): Article 1 must be maintained because it sets out the scope and subject matter of the P2B Regulation, which are necessary elements for the proper application of the other provisions that remain in force.
(a) Article 2, point (1);	BE (Drafting suggestions): (a) Article 2, point**s** ~~(5);~~ **(1) to (10) and (13);** BE (Comments): To ensure the legal certainty and coherence of the remaining provisions of the P2B Regulation, it is necessary to maintain certain definitions set out in Article 2.

Presidency first compromise text	Drafting suggestions and Comments
	We have identified that the definitions in points (11) and (12) can be repealed, as they are not used in the retained provisions of the P2B Regulation. IE (Drafting suggestions): (a) Article 2 IT (Drafting suggestions): (a) **(b)** Article 2, point**s** (5); **(1) to (10) and (13);** IT (Comments): To ensure the legal certainty and coherence of the remaining provisions of the P2B Regulation, it is necessary to maintain certain definitions set out in Article 2. We have identified that the definitions in points (11) and (12) can be repealed, as they are not used in the retained provisions of the P2B Regulation. NL (Drafting suggestions): (a) Article 2, point**s** ~~(5);~~ **(1) to (10) and (13);** NL (Comments): To ensure the legal certainty and coherence of the remaining provisions of the P2B Regulation, it is necessary to maintain certain definitions set out in Article 2.

Presidency first compromise text	Drafting suggestions and Comments
	We have identified that the definitions in points (11) and (12) can be repealed, as they are not used in the retained provisions of the P2B Regulation
(b) Article 2, point (2);	BE (Drafting suggestions): ~~(b) Article 2, point (2);~~ IE (Drafting suggestions): ~~(b) Article 2, point (2);~~ (b) Article 3 IT (Drafting suggestions): ~~(b) Article 2, point (2);~~ NL (Drafting suggestions): ~~(b) Article 2, point (2);~~
	CZ (Drafting suggestions): **(x) Article 2, point (3);**

Presidency first compromise text	Drafting suggestions and Comments
	(x) Article 2, point (4); CZ (Comments): CZ to 2(3): The definition of a provider of online intermediation services is essential for interpreting the provisions retained in the P2B Regulation. This includes Articles 4 and 11 of the P2B Regulation that are to be retained under Commision proposal. Repealing the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (3) of the P2B Regulation shall be retained. CZ to 2(4): The term "consumer" is included in the obligations that CZ proposes to retain (e.g., Article 3(4), point (b) of the P2B Regulation), but also in the definition of a business user. Repealing the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (4) of the P2B Regulation shall be retained.
(c) Article 2, point (5);	BE (Drafting suggestions): ~~(c) Article 2, point (5);~~ CZ (Comments): CZ: The term “online search engine” is included in the definition of the term “provider of online search engines”. The term “provider of online search

Presidency first compromise text	Drafting suggestions and Comments
	engines" is included in obligations that CZ proposes to retain (e.g., Article 5(2) of the P2B Regulation). If the obligations proposed by CZ were retained, the repeal of the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (5) of the P2B Regulation shall be retained. IE (Drafting suggestions): ~~(c) Article 2, point (5);~~ (c) Article 4 IT (Drafting suggestions): ~~(c) Article 2, point (5);~~ NL (Drafting suggestions): ~~(c) Article 2, point (5);~~
	BE (Drafting suggestions): **(ca) Article 3;** BE (Comments): Article 3 contains material obligations for platforms. Without Article 3.2, business users will no longer be informed before terms and conditions are changed and they will lose the right to terminate the agreement on these grounds. This harms the business user's position in their relation to the platform by weakening contractual transparency and predictability. In addition to the material obligation of Article 3(2), the transparency obligations set out in Article 3 offer considerable protection to business users, particularly since non-compliant terms and conditions are

Presidency first compromise text	Drafting suggestions and Comments
	automatically null and void. The repeal of Article 3 would remove an important safeguard for business users against arbitrary enforcement, thereby depriving them of the right to be informed in advance, in a clear and comprehensible manner, of the potential conditions under which the service may be restricted, irrespective of the size of the platform. CZ (Drafting suggestions): **(x) Article 2, point (6);** **(x) Article 2, point (7);** **(x) Article 2, point (10);**

Presidency first compromise text	Drafting suggestions and Comments
	(x) Article 2, point (13); **(x) Article 3(1), point (b);**

Presidency first compromise text	Drafting suggestions and Comments
	(x) Article 3(2); **(x) Article 3(3);** **(x) Article 3(4);** CZ (Comments): CZ to 2(6): The term "provider of online search engines" is included in obligations that CZ proposes to retain (e.g., Article 5(2) of the P2B Regulation). If the obligations proposed by CZ were retained, the repeal of the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (6) of the P2B Regulation shall be retained. CZ to 2(7): The term "corporate website user" is included in obligations that CZ proposes to retain (e.g. Article 5(3) of the P2B Regulation). If the obligations proposed by CZ were retained, the repeal of the definition would

Presidency first compromise text	Drafting suggestions and Comments
	create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (7) of the P2B Regulation shall be retained. CZ to 2(10): The term "terms and conditions" is included in obligations that CZ proposes to retain (e.g. Article 3(1), point (b) of the P2B Regulation) or even in obligations that Comission proposes to retain (e.g. Article 11 of the P2B Regulation). Repealing the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (10) of the P2B Regulation shall be retained. CZ to 2(13): The term "durable medium" is included in obligations that Comission proposes to retain (e.g. Article 4 of the P2B Regulation). Repealing the definition would create unnecessary legal uncertainty, and it is therefore proposed that Article 2, point (13) of the P2B Regulation shall be retained. CZ to 3(1(b)): proposes that the obligation of providers of online intermediation services to ensure that their terms and conditions are easily available to business users, including in the pre-contractual stage, shall be retained. Compared to Article 14(1) of the DSA Regulation, this obligation applies both to the pre-contractual stage and to a wider range of information. This requirement is on its own essential for the purposes of transparency and the principle of good faith, e.g. with regard to access to data (which shall be repealed by the Commission's proposal but generally permitted in accordance with the principle of contractual freedom).

Presidency first compromise text	Drafting suggestions and Comments
	CZ to 3(2): CZ proposes to retain principle of absolute invalidity for both Article 3(1)(b) and Article 3(2) of the P2B Regulation. The invalidity of terms and conditions or their changes is an important private law instrument that business users can use to protect themselves against violations of the P2B Regulation by online intermediary service providers. CZ to 3(4): CZ proposes that the obligations of providers of online intermediary service regarding changes to their terms and conditions, shall be retained. Protecting business users from arbitrary changes to terms and conditions is essential, this is apparent also from the fact, that Commission plans to not repeal Article 4 of the P2B Regulation. Otherwise, business users would not be directly informed of the changes in terms and conditions, which would have an adverse effect on their provision of goods and services through the provider's service. If we would repeal obligation to inform users about changes in their terms and conditions in advance, platforms could utilize changing of their terms and conditions for the purpose of restriction, suspension or termination of user accounts, which is something what Article 4 of the P2B Regulation strives to prevent. However, it is also appropriate to retain the exemptions from this obligation under Article 3(4) of the P2B Regulation and to allow providers of online intermediation service to change their terms and conditions rapidly in exceptional circumstances. FI

Presidency first compromise text	Drafting suggestions and Comments
	(Drafting suggestions): **(ca) Article 2, point (10);** **(cb) Article 3;** FI (Comments): Finland considers it essential to ensure transparent and fair contractual relationships between business users and online platform companies also in the future. Transparent contracts and predictable markets enable especially SMEs to create economic growth and stay competitive. Finland considers that the key impact from repealing the P2B Regulation would be that **the service provider is not obliged to notify in advance** of any change of the service to the business user. To ensure legal certainty for business users when operating on online platforms of all sizes, **Finland proposes that also Article 3 of the P2B Regulation should be retained until 2032**. In addition, the Commission should commit to examining how especially **the articles 3(2) and 4(2) may be included in the remaining legislation, for instance to the Digital services Act (DSA), before 2032** when the transition period ends. IT (Drafting suggestions): **(c) Article 3;** IT (Comments): Article 3 contains material obligations for platforms. Without Article 3.2, business users will no longer be informed before terms and conditions are changed and they will lose the right to terminate the agreement on these

Presidency first compromise text	Drafting suggestions and Comments
	grounds. This harms the business user's position in their relation to the platform by weakening contractual transparency and predictability. In addition to the material obligation of Article 3(2), the transparency obligations set out in Article 3 offer considerable protection to business users, particularly since non-compliant terms and conditions are automatically null and void. The repeal of Article 3 would remove an important safeguard for business users against arbitrary enforcement, thereby depriving them of the right to be informed in advance, in a clear and comprehensible manner, of the potential conditions under which the service may be restricted, irrespective of the size of the platform. NL (Drafting suggestions): **(ca) Article 3;** NL (Comments): Article 3 contains material obligations for platforms. Without Article 3.2, business users will no longer be informed before terms and conditions are changed and they will lose the right to terminate the agreement on these grounds. This harms the business user's position in their relation to the platform by weakening contractual transparency and predictability. In addition to the material obligation of Article 3(2), the transparency obligations set out in Article 3 offer considerable protection to business users, particularly since non-compliant terms and conditions are automatically null and void. The repeal of Article 3 would remove an important safeguard for business users against arbitrary enforcement, thereby depriving them of the right to be informed in advance, in a clear and

Presidency first compromise text	Drafting suggestions and Comments
	comprehensible manner, of the potential conditions under which the service may be restricted, irrespective of the size of the platform.
(d) Article 4;	IE (Drafting suggestions): (d) Article ~~4;~~ 11
	BE (Drafting suggestions): **(da) Article 5;** **(db) Article 7;** **(dc) Article 10 ;** BE (Comments): Article 5 must remain in force because national authorities play a crucial role in addressing ranking-related complaints from business users, and a notable number of requests based on this article has been received at the national level. Repealing Article 5 would risk reducing the accessibility and effectiveness of redress for SMEs operating on platforms. Belgium also asks to maintain Article 7 as it provides SMEs with insight into the various forms of differentiated treatment they may be subjected to and it enables authorities, including those under the DMA and competition law, to detect and address such practices. Without this provision, platforms are free to put business users at a disadvantage where they compete with the platform's own products and services, or with other business users controlled by the platform, without disclosure. Again, it is important to note that some Member States have received a notable number of Article 7 complaints and tip-offs.

Presidency first compromise text	Drafting suggestions and Comments
	In addition, we consider Article 10 should also be maintained given the fact that as most platforms are not gatekeepers, repealing Article 10 will allow them to impose parity clauses without transparency. They will not need to provide any justification and prospective business users will not know such restrictions exist. This lack of transparency will make it significantly more difficult for authorities to gain insight into these practices and for affected business users to challenge them. CZ (Drafting suggestions): **(x) Article 5(2), (3), (4), (5), (6)**

Presidency first compromise text	Drafting suggestions and Comments
	(x) Article 8, point (b); CZ (Comments): CZ proposes that the obligations of providers of online search engines in relation to ranking according to Article 5(2) to (6) of the P2B Regulation, shall be retained. These obligations are set out exclusively in the P2B Regulation and do not overlap with, for example, Article 27 of the DSA Regulation, because this provision of the DSA Regulation applies only to "mid-size" providers of online platforms, not providers of online search engines. Online search engines serve as gateways to information available on the internet, and therefore the repeal of these obligations may have an indirect impact on human rights of business users such as freedom of expression or free enterprise. CZ to 8(b): CZ proposes that the obligation of provider of online intermediation services to include information on the conditions under which business users can terminate the contractual relationship with the provider to their terms and conditions, shall be retained. It is very important that business users are informed of the circumstances under which they may terminate the use of a service in the case of unilaterally determined terms and conditions. Otherwise, providers of online intermediation services may, contrary to the principle of good faith, completely omit the option for business users to terminate the service and not

Presidency first compromise text	Drafting suggestions and Comments
	allow them to do so. Or they could charge users with additional costs or fines. While this practice could be, in theory, dealt with through the civil proceedings, considering the will of small business users to engage in lengthy proceedings, public oversight should be considered as quite useful in this case. It is also important to note that this obligation is not explicitly laid down in any other Union legislation, as, for example, Article 14(1) of the DSA Regulation only applies to grounds for restricting services by providers of online intermediation services. IT (Drafting suggestions): **(da) Article 5;** **(db) Article 7;** **(dc) Article 10 ;** IT (Comments): Article 5 must remain in force because national authorities play a crucial role in addressing ranking-related complaints from business users, and a notable number of requests based on this article has been received at the national level. Repealing Article 5 would risk reducing the accessibility and effectiveness of redress for SMEs operating on platforms. ITALY also asks to maintain Article 7 as it provides SMEs with insight into the various forms of differentiated treatment they may be subjected to and it enables authorities, including those under the DMA and competition law, to detect and address such practices. Without this provision, platforms are free to put business users at a disadvantage where they compete with the platform's own products and services, or with other business users controlled

Presidency first compromise text	Drafting suggestions and Comments
	by the platform, without disclosure. Again, it is important to note that some Member States have received a notable number of Article 7 complaints and tip-offs. In addition, we consider Article 10 should also be maintained given the fact that as most platforms are not gatekeepers, repealing Article 10 will allow them to impose parity clauses without transparency. They will not need to provide any justification and prospective business users will not know such restrictions exist. This lack of transparency will make it significantly more difficult for authorities to gain insight into these practices and for affected business users to challenge them. NL (Drafting suggestions): **(da) Article 5;** **(db) Article 7;** **(dc) Article 10 ;** NL (Comments): Article 5 must remain in force because national authorities play a crucial role in addressing ranking-related complaints from business users, and a notable number of requests based on this article has been received at the national level. Repealing Article 5 would risk reducing the accessibility and effectiveness of redress for SMEs operating on platforms. The Netherlands also asks to maintain Article 7 as it provides SMEs with insight into the various forms of differentiated treatment they may be

Presidency first compromise text	Drafting suggestions and Comments
	subjected to and it enables authorities, including those under the DMA and competition law, to detect and address such practices. Without this provision, platforms are free to put business users at a disadvantage where they compete with the platform's own products and services, or with other business users controlled by the platform, without disclosure. Again, it is important to note that the ACM received a notable number of Article 7 complaints and tip-offs. In addition, we consider Article 10 should also be maintained given the fact that as most platforms are not gatekeepers, repealing Article 10 will allow them to impose parity clauses without transparency. They will not need to provide any justification and prospective business users will not know such restrictions exist. This lack of transparency will make it significantly more difficult for authorities to gain insight into these practices and for affected business users to challenge them.
(e) Article 11;	IE (Drafting suggestions): (e) Article ~~11~~ 12
(f) Article 15.	
	BE (Drafting suggestions): **(fa) Article 19** BE (Comments): Article 19 must remain in force to maintain coherence of the Regulation following its partial repeal. We believe its removal will lead to ambiguity and legal uncertainty. CZ

Presidency first compromise text	Drafting suggestions and Comments
	(Drafting suggestions): **(x) Article 19:** **X. By way of derogation from paragraph 1, the Regulation 2019/1150/EU is amended as follows:** **1. Article 5(3) is replaced by the following:** **'3. Where the main parameters include the possibility to influence ranking against any direct or indirect remuneration paid by business users or corporate website users to the respective provider, that provider shall also set out a description of those possibilities and of the effects of such remuneration on ranking in accordance with the requirements set out in paragraph 2** **2. Article 5(5) is replaced by the following:** **'5. The descriptions referred to in paragraphs 2 and 3 shall be sufficient to enable the business users or corporate website users to obtain an adequate understanding of whether, and if so how and to what extent, the ranking mechanism takes account of the following:**

Presidency first compromise text	Drafting suggestions and Comments
	(a) the characteristics of the goods and services offered to consumers through the online search engine; **(b) the relevance of those characteristics for those consumers;** **(c) the design characteristics of the website used by corporate website users.** **3. Article 5(6) is replaced by the following:** **'6. Providers of online search engines shall, when complying with the requirements of this Article, not be required to disclose algorithms or any information that, with reasonable certainty, would result in the enabling of deception of consumers or consumer harm through the manipulation of search results. This Article shall be without prejudice to Directive (EU) 2016/943.** CZ (Comments): CZ to art. 19: Article 19 of the P2B Regulation establishes the temporal scope of application of the P2B Regulation. That is one of the essential requirements for the validity of a legal norm, and therefore it is necessary to consider whether it is possible to repeal the provision without replacing it in adequate manner. CZ: Those proposed amendments to Article 5 of the P2B Regulation are necessary in order to avoid references to Article 5(1) of the P2B Regulation, which is to be repealed, thereby preventing legal uncertainty. Otherwise, the provisions of Article 5(2) to (6) of the P2B Regulation would refer to legal obligations that have already been repealed.

Presidency first compromise text	Drafting suggestions and Comments
	IT (Drafting suggestions): **(fa) Article 19** IT (Comments): Article 19 must remain in force to maintain coherence of the Regulation following its partial repeal. We believe its removal will lead to ambiguity and legal uncertainty. NL (Drafting suggestions): **(fa) Article 19** NL (Comments): Article 19 must remain in force to maintain coherence of the Regulation following its partial repeal. We believe its removal will lead to ambiguity and legal uncertainty.
Article 11	
Final provisions	
This Regulation shall enter into force on the third day following that of its publication in the Official Journal of the European Union.	
Deviating from paragraph 3, Article 5(2) shall enter into application 6 months after the publication in the Official Journal of the European Union.	

Presidency first compromise text	Drafting suggestions and Comments
Article 3(8), points (a) to (c), Articles 6 (2) and (3) and 7 to 9, shall enter into application 18 months from the entry into force of this Regulation. Deviating from the first sentence, where the Commission finds in its assessment pursuant to Article 23a (7) of Directive (EU) 2022/2555 that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality, the obligations to report via the single-entry point set out in Article 23(4) of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU) 2022/2554, and Article 15(1) of Directive (EU) 2022/2557 shall enter into application 24 months from the entry into force of this Regulation.	
This Regulation shall be binding in its entirety and directly applicable in all Member States.	